高等教育质量工程信息技术系列示范教材

计算机网络教程

（第2版）

张基温 编著

清华大学出版社

高等教育质量工程信息技术系列示范教材

计算机网络教程

（第2版）

张基温　编著

清华大学出版社
北　京

内 容 简 介

本书是为应用型本科院校计算机网络课程编写的教材，书中贯穿了“以协议为核心，以应用为目的”的思想，采用了既有理论讲解又有实践跟进的全新编写体系。全书共分 7 章，各章内容分别是计算机网络概述、数据通信的基础、TCP/IP 与网络互连、Internet 应用、局域网组网技术、接入网技术以及网络安全。

本书从实用性出发而又不忽视基本理论，强调基础而又贴近主流网络技术，内容经典而又紧跟知识变化的步伐。为方便学习，书中配有大量的操作插图，每章都配有一定量的经典实验和习题。

本书既可作为高等院校信息类专业的计算机网络教材，也可作为高等院校非网络专业的本科教材或各类计算机培训机构的教材。

图书在版编目（CIP）数据

计算机网络教程/张基温编著. —2 版. —北京：清华大学出版社，2018
（高等教育质量工程信息技术系列示范教材）
ISBN 978-7-302-49011-1

Ⅰ. ①计… Ⅱ. ①张… Ⅲ. ①计算机网络– 高等学校– 教材 Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字（2017）第 292541 号

责任编辑：白立军
封面设计：常雪影
责任校对：胡伟民
责任印制：沈 露

出版发行：清华大学出版社
网 址：http://www.tup.com.cn, http://www.wqbook.com
地 址：北京清华大学学研大厦 A 座 **邮 编：**100084
社 总 机：010-62770175 **邮 购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn,010-62795954
印 装 者：北京泽宇印刷有限公司
经 销：全国新华书店
开 本：185mm×260mm **印 张：**20.75 **字 数：**510 千字
版 次：2017 年 1 月第 1 版 2018 年 1 月第 2 版 **印 次：**2018 年 1 月第 1 次印刷
印 数：1～1500
定 价：49.00 元

产品编号：075144-01

前　　言

当今社会处在信息时代，网络时代。不分专业，不分职业，不分老少，不分民族，不分国籍，不分地域，人人、处处、时时、刻刻，都有人工作在网络中，学习于网络中，交易于网络中，交流于网络中，甚至沉溺于网络中。网络神奇而又普通，虚拟而又实在，强烈地激发着亿万人了解它的奥秘、提升它的愿望。在学校中，也被越来越多的专业将之列为教学的内容。

但是，学习计算机网络却不是一件容易的事情。从学科方面看，它涉及数学、物理、机械、电气、信息、管理；从教学形式上看，它涉及课堂理论、实验研究、工程实践；从内容上看，它还在不断发展，推陈出新。难怪问到已经学过这门课的同学有何感想时，多数人的回答是：一大堆概念；甚至还有相当多的同学对这门课感到茫然。

这门课确实难教，这门课的教材也确实难写。不过，这些难度也给了笔者一些改革与探索的冲动：从实用性出发而又不忽视基本理论，强调基础而又贴近主流网络技术，内容经典而又紧跟知识变化的步伐，在面对知识的很强离散性时还需让学习者便于梳理。几十年来虽然在多家出版社推出过不同结构、面向不同对象的教材，但都有继续改进的必要。

此次，本书作为清华大学出版社“高等教育质量工程信息技术系列示范教材”系列中的一种书出版，笔者认真总结了以前各种版本的优缺点，确定了“以协议为主线，贴近实际，紧跟发展”的编写思路，目的在于让学习者抓牢协议这根网络的“神经”，学以致用，提高学习兴趣。

在这次修订中，张展赫参加了部分写作，并由张秋菊、赵忠孝、史林娟、张展为、董兆军、张友明、陈觉、戴璐分别制图、校对。此外，本书在写作过程中，参考了不少其他作品，已经在参考文献中加以说明。还有一些是网上的佚名作者，这部分资料，无法在参考文献中说明。在本书出版之际谨向这些为本书出版做出了贡献的人们致以衷心谢意。

本书作为一种新体系的作品，难免存在这样或那样的问题，还请有关专家和各位读者多多批评并不吝赐教。

编　者

2017 年 5 月

目　　录

第 1 章　计算机网络基础

计算机网络是计算机技术和通信技术密切结合的产物，它代表了当代计算机体系结构发展的一个极其重要的方向。本章介绍有关计算机网络的基本概念和技术，为后续学习奠定基础。

1.1　计算机网络的基本概念

1.1.1　计算机网络及其功能

1. 计算机网络的定义

关于“计算机网络”，一直没有严格意义上的统一定义，而且随着计算机技术和通信技术的发展，其内涵也在不断地发展变化。从广义的角度讲，计算机网络是计算机技术与通信技术相结合，实现信息传送和资源共享为目的的系统集合。

美国信息处理学会联合会认为，计算机网络是以能够相互共享资源（硬件、软件、数据）的方式连接起来的，并各自具备独立功能的计算机系统的集合。

本书给出如下定义：计算机网络是将处于不同地理位置且相互独立的计算机或设备（比如打印机、传真机等），在网络协议和网络操作系统的控制下，利用传输介质和通信设备连接起来，从而实现信息传递和资源共享为主要目的的系统集合。如图 1.1 所示为一个计算机网络。

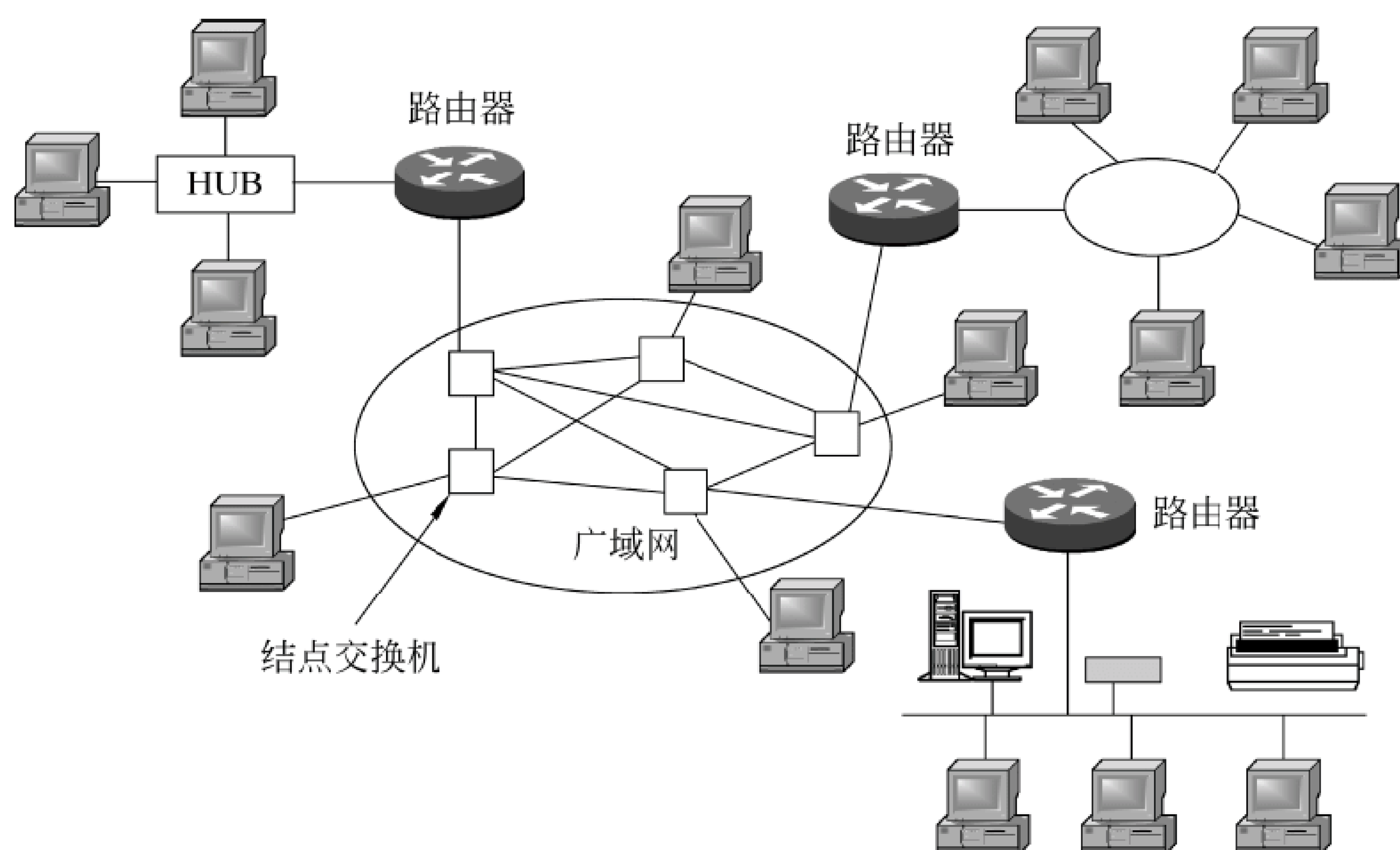


图 1.1　计算机网络

在图 1.1 中，路由器是不同网络之间的联接设备，交换机是一个网络中不同的数据传输

链路之间的连接设备。

2. 计算机网络的功能

现今，人们非常迷恋计算机网络，那到底计算机网络给人们带来了哪些好处？换句话说，计算机网络主要为用户提供了哪些功能呢？

1）数据传输

这里的数据指的是数字、文字、声音、图像、视频信号等媒体信息的计算机表示。在计算机世界里，一切事物都可以用 0 和 1 这两个数字表示出来。计算机网络使得各种媒体信息通过通信线路进行传输。数据传输是计算机网络各种功能的基础，有了数据传输，才会有资源共享。

2）资源共享

资源包括硬件、软件和数据。硬件为各种处理器、存储设备、输入/输出设备等，可以通过计算机网络实现这些硬件的共享，如打印机、外存空间等。软件包括操作系统、应用软件、驱动程序等，可以通过计算机网络实现这些软件的共享，如多用户的网络操作系统、应用程序服务器。数据包括用户文件、配置文件、数据文件、数据库等，可以通过计算机网络实现这些数据的共享，如通过网上邻居复制文件和网络数据库。通过共享能使资源发挥最大的作用，同时节省成本，提高效率。

3）负载均衡

在有很多台计算机的环境中，这些计算机需要处理的任务可能不同，经常有忙闲不均现象的出现。有了计算机网络，可以通过网络调度来协调工作，把“忙”的计算机上的部分工作交给“闲”的计算机去做，还可以把庞大的科学计算或复杂信息处理问题交给几台联网的计算机，由它们协调配合来完成。分布式信息处理、分布式数据库等就是利用计算机网络来实现负载均衡最好的例子。

4）网络服务

现在，风靡全球的电子邮件、文件传输、网络会议、博客、微博、微信、电子商务、电子政务、物联网等都是计算机网络的产物，它们给人们的生活、学习和娱乐带来极大的方便。有了计算机网络，实时控制系统才有了保障，军事设施、道路交通设施等才能在无人值守的情况下准确无误地运作。伴随着计算机网络新技术的不断出现，人们的生活、工作和学习会越来越方便。

1.1.2 计算机网络两级模型：资源子网+通信子网

计算机网络是计算机技术与通信技术相结合的产物，从功能上说，计算机网络系统可以分为通信子网和资源子网两大部分，如图 1.2 所示。通信子网提供通信，即数据传输的能力。资源子网提供网络上的资源（主计算机——涉及软硬件处理能力和数据）以及访问能力（终端及其终端控制器）。

1. 资源（用户）子网

资源子网（也称用户子网）负责全网的数据处理业务，向全网用户透明地提供所

需的网络资源和网络服务。这里所说的“透明”，是指用户可以不涉及资源传输和处理的细节。

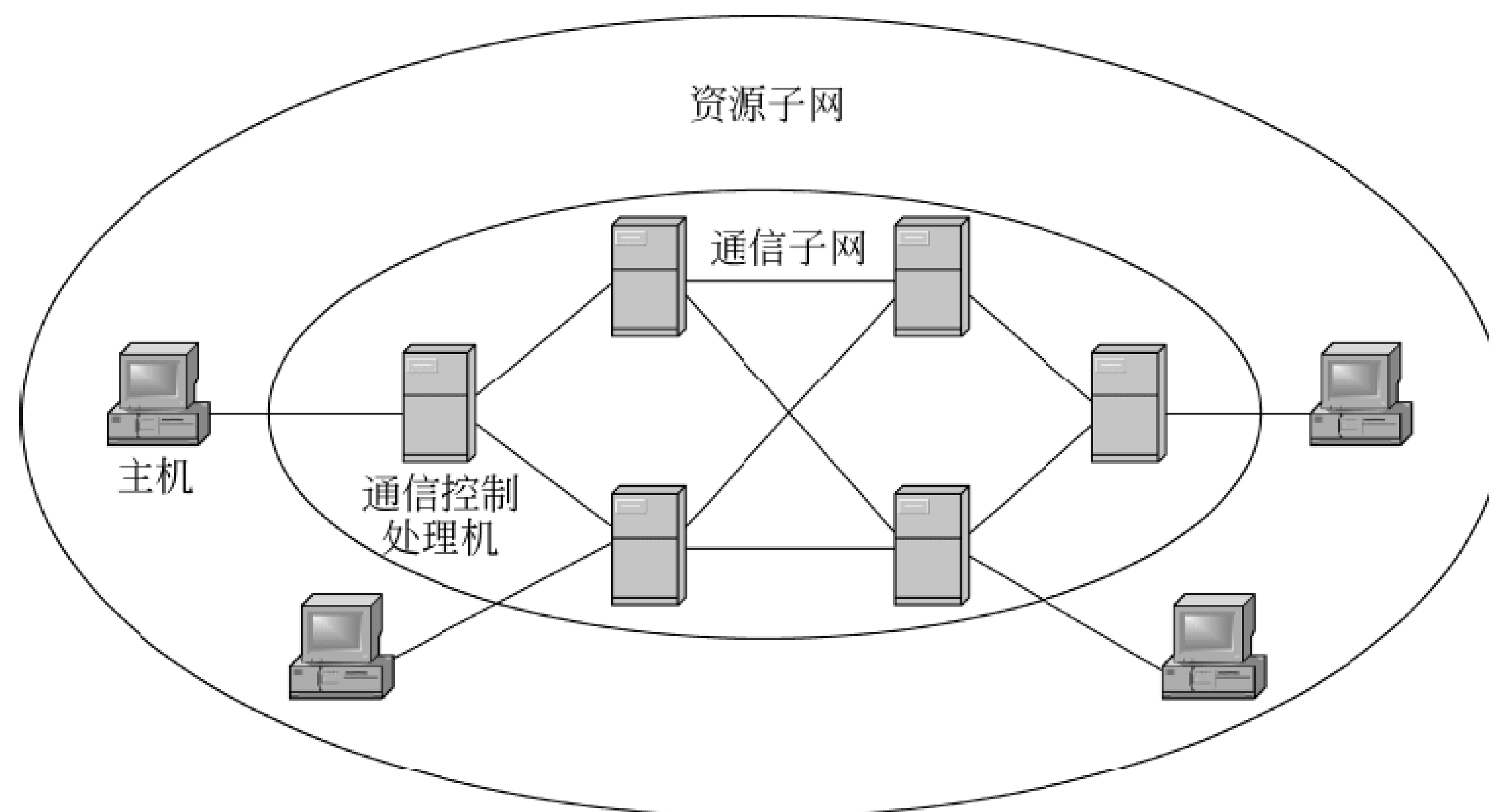


图 1.2　通信子网与资源子网

资源子网由一些资源单元组成，如主机（Host）、终端设备（Terminal，T）控制器、各种外部设备以及相关软件资源和数据资源。

主机在网络中负责数据处理、网络控制并执行网络协议。为了能在网络上工作，主机中必须安装如下两类软件：

（1）主机操作系统——管理计算机本身的资源。

（2）网络操作系统（Network Operating System，NOS），支持不同主机系统之间的用户通信、实现网络中资源共享，向用户提供统一、方便的网络接口。

终端是用户进行网络操作时所使用的设备，也可以看成是计算机系统组成部分。其种类很多，如显示终端（Display Terminal，DT）、交互终端 CRT、智能终端（Intelligent Terminal，IT）、图形终端（Graphic Terminal，GT）、批作业或远程终端（batch or Remote Job Entry terminal，RJE）等。

2．通信子网

通信子网由通信控制处理机（Communication Control Processor，CCP）、通信链路以及信号变换器等组成，承担全网的数据传输和交换等任务，为资源子网提供透明的数据传输服务。

1.1.3　计算机网络的基本类型

计算机网络是一种复杂的系统。人们对于复杂系统的认识，一开始只能像盲人摸象，认识一个片面，但若能从不同的角度触摸几次，认识就会趋向全面。关于计算机网络的类型，就是从不同角度观察进行的区分，例如：

- 按地理覆盖范围，可以分为广域网、城域网、局域网和个人网。
- 按拓扑结构，可以分为总线型、星形、树形、网状等。
- 按网络中计算机之间的关系，可以分为对等网和客户机-服务器网。

- 按使用权限，可以分为公网和私网、外网和内网等。
- 按业务范围，可以分为校园网、企业网、金桥网、教育科研网、经济网、科技网、医卫网、电话网以及广播电视网等。
- 按开发者名称分类，如 IBM 网、ARPANet、ChinaNet、微软网等。
- 按采用的网络技术分类，如 x.25、ALOHA、DDN、帧中继、ISDN、ATM、TCP/IP 等。
- 按所运行的操作系统分类，如 UNIX 网、Linux 网、Windows NT、Novell NetWare 等。
- 按采用的传输介质分类，如铜线网络、无线网、光纤网等。

下面较详细地介绍对后继学习影响较大的前两种分类方法。

1. 按网络覆盖的地理范围分类

一般将计算机网络分为 4 类：局域网、城域网、广域网、个人网。

1）局域网

局域网（Local Area Network，LAN）覆盖范围一般在几千米以内，通常属于一个单位、一个部门或一个实验室，或在一幢大楼、一个校园、一个园区内。局域网的本质特征是作用范围小、传输速率高（通常为 10Mbps～10Gbps）、延迟小、可靠性高。再加上 LAN 具有低成本、应用广、组网方便、使用灵活等特点，深受广大用户的欢迎。因此，LAN 是目前发展最快、最活跃的一个分支。

2）城域网

城域网（Metropolitan Area Network，MAN）原本指的是介于局域网与广域网之间的大范围高速网络，其作用范围在一个城市之内，从几 km 到几十 km。目前，随着网络技术的迅速发展，局域网、城域网和广域网的界限已经变得十分模糊。

3）广域网

广域网（Wide Area Network，WAN）所覆盖的地理范围一般为几百 km 到几千 km，因为其覆盖的范围广，故称其为广域网，也称为远程网。它一般可以覆盖几个城市、地区，甚至国家、洲或全球。这类网络出现得最早，其骨干网络一般是公用网，传输速率较高，能够达到若干 Gbps。

4）个人网

个人局域网（Personal Area Network，PAN）是在计算机网络大为普及、各种短距离无线通信技术不断发展的情况下出现的一种计算机网络形态。其特点是用无线电或红外线代替传统的有线电缆，实现个人信息终端的智能化互联，组建个人化的信息网络，适合于家庭与小型办公室的应用场合；其主要应用范围包括微信、QQ 以及信息电器互联与信息自动交换等。

PAN 的实现技术主要有 Bluetooth、Wi-Fi、IrDA、Home RF、ZigBee、WirelessHart 与 UWB（Ultra-Wideband Radio）。

2. 计算机网络的拓扑结构

为了研究计算机网络物理上的连通性，可以将网络设备抽象为一些点，称为结点；把传输介质抽象为线，称为链路，所形成几何图形称为网络拓扑结构。

1）星形拓扑

如图 1.3（a）所示，星形拓扑是网络中的各结点通过点到点的方式连接到一个中心结点（又称中央转接站，一般是集线器或交换机）上，中心结点控制全网的通信，向目的结点传送信息。

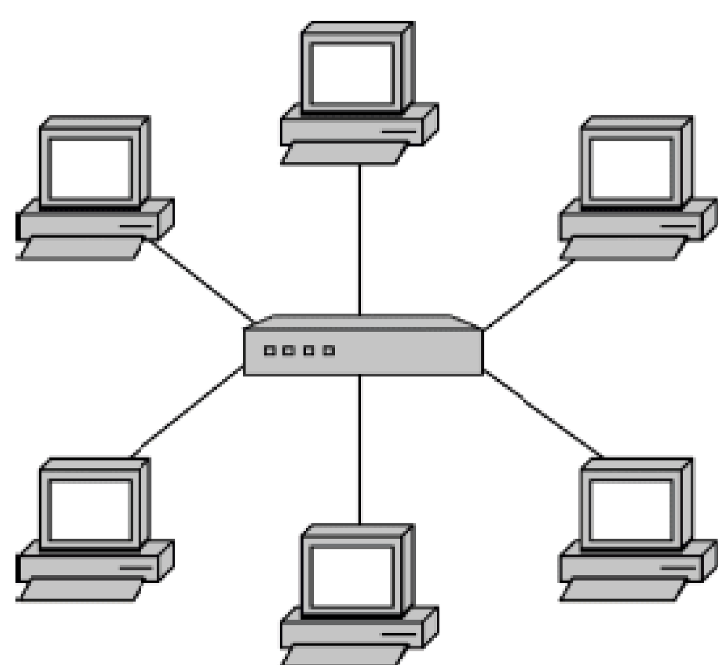
星形拓扑便于集中控制，任何两台计算机之间的通信都要通过中心结点来转接，网络延迟时间较小，传输误差较低，也易于维护和管理。但是要求中心结点必须具有极高的可靠性，因为中心结点一旦损坏，整个系统便趋于瘫痪。对此，中心结点通常采用双机热备份，以提高系统的可靠性。此外，其通信线路须专用，电缆成本高。

2）总线型拓扑

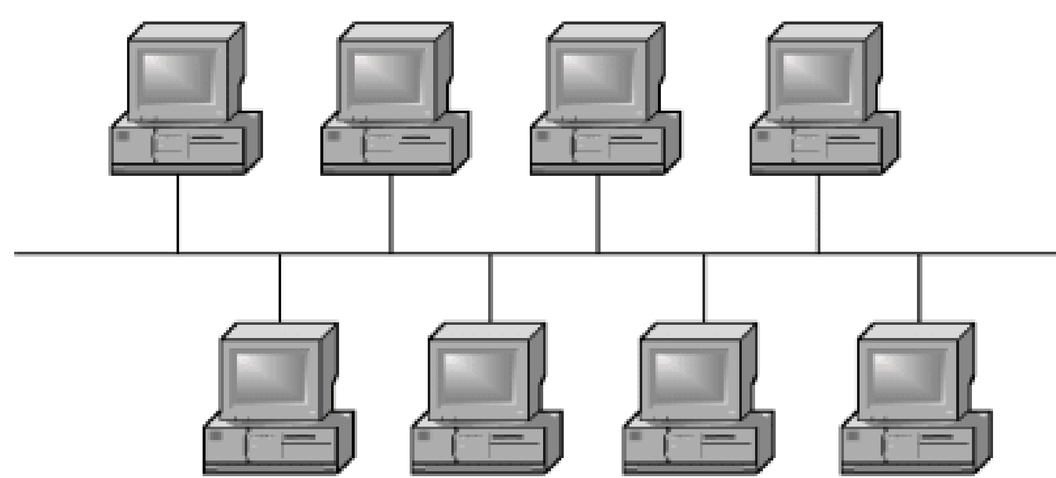
如图 1.3（b）所示，在总线型拓扑结构中，网络中的所有结点都通过接口串接在一个被叫作总线的单根传输线路上。每一个结点发送的信息都必须在总线上传输，且能被其他结点所接收。这种结构连接简单、易于安装、成本费用低。但是，在任何一个时间点上，网中只能有一个结点向外发送消息；否则产生冲突。同时为了防止信号到达线缆的端点时产生反射信号，引起与后续信号的冲突，必须在线缆的两端安装终结器以吸收端点信号。此外，这种网络维护困难，总线一旦出现断点，整个网络将瘫痪，而且故障点很难查找。

3）环形拓扑

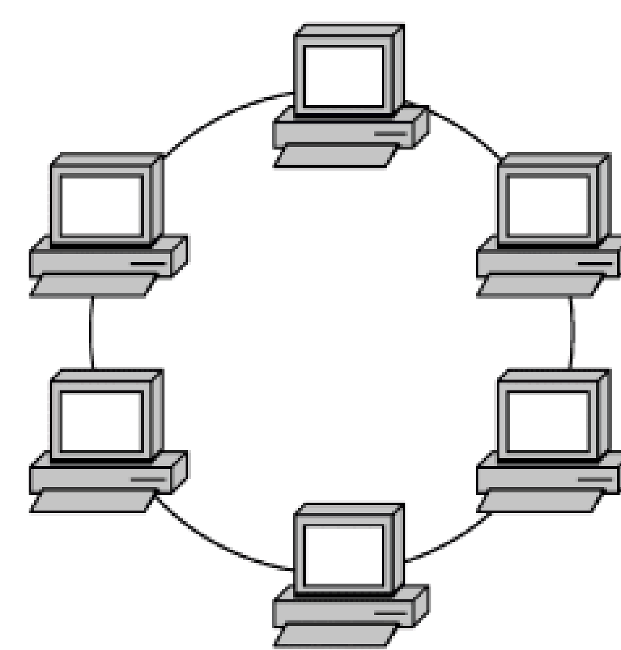
如图 1.3（c）所示，将总线的首尾相连，就形成环形结构。为了避免环路上同时发送数据引起的冲突，在网络中要运行一种特殊的信号——令牌，令牌按顺时针方向传输。当某台计算机要发送信息时，必须先捕获令牌，再发送信息；发送信息后再释放令牌。与总线结构相似，这种网络实现简单，且传输介质适合采用光纤，以实现高速连接。但这种结构也存在致命的弱点，即网中任何一个结点出现故障就会导致全网瘫痪。



(a) 星形拓扑结构



(b) 总线型拓扑结构



(c) 环形结构

图 1.3　计算机网络基本拓扑结构（1）

4）树形拓扑

如图 1.4（a）所示，树形拓扑结构是星形拓扑结构的拓展，它采用层次化的结构，具

有一个根结点和多层分支结点。树形网络中除了叶子结点外，所有分支结点都是转发结点。它的各个结点按层次进行连接，数据的交换主要在上下结点间进行。树形结构属于集中控制式网络，适用于分级管理的场合，如图 1.6 所示的三层结构也是三级层次。

树形拓扑结构比较简单，成本低。扩充结点方便灵活。但是对根结点（相当于星形拓扑中的中心结点）的依赖性大，一旦根结点出现故障，将导致全网不能工作；此外电缆成本高。

5）网状拓扑

如图 1.4（b）所示，网状拓扑结构的特点是，任何一个结点至少有两条线路与其他结点相连。在极端情况下，网络中所有结点都互相连结形成全连网状结构，如图 1.4（c）所示。这种结构的优点是不存在瓶颈结点和瓶颈链路。由于结点之间有许多条路径相连，可靠性高；也便于选择最佳路径，减少时延，改善流量分配，提高网络性能；但结构复杂，不易管理和维护，线路成本高；适用于大型广域网。

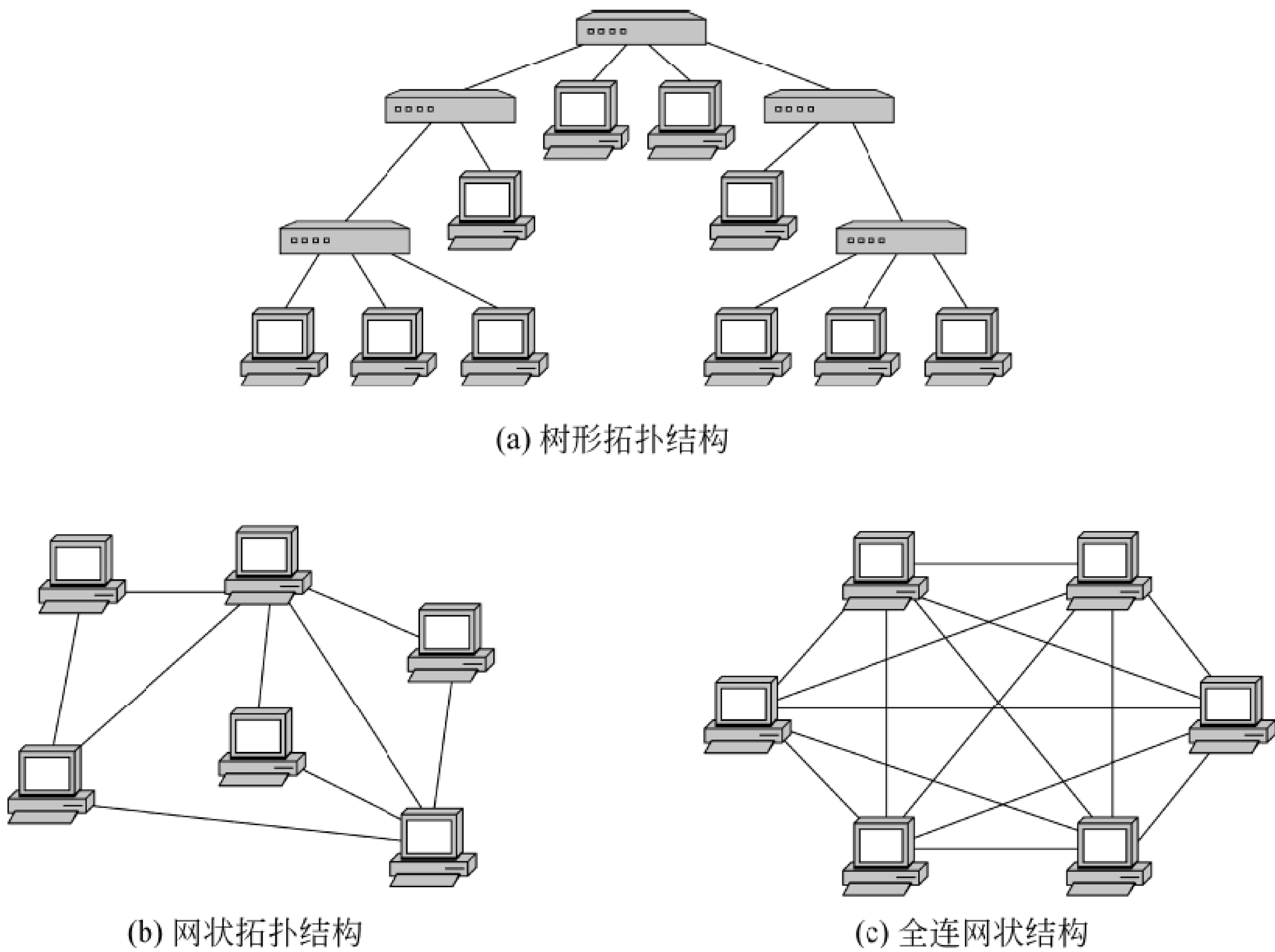


图 1.4　计算机网络基本拓扑结构（2）

6）混合式拓扑

目前局域网都不采用单纯的某一种网络拓扑结构，而是根据具体需要和环境将几种基本网络结构进行综合。常见的混合式网络拓扑结构有星网型（如图 1.1 所示）、星总型结构和星树形结构等。也有 3 种以上基本结构的结合型，如图 1.5 所示。

7）蜂巢式拓扑

蜂巢拓扑结构是无线网络中常用的结构。在无线网络中，建有许多基站，每个基站充当星形结构中的中心结点，控制其辐射范围内的用户无线设备。各基站的辐射区域形成如图 1.6 所示的蜂巢形状。蜂巢式网络拓扑适用于城市网、校园网、企业网。

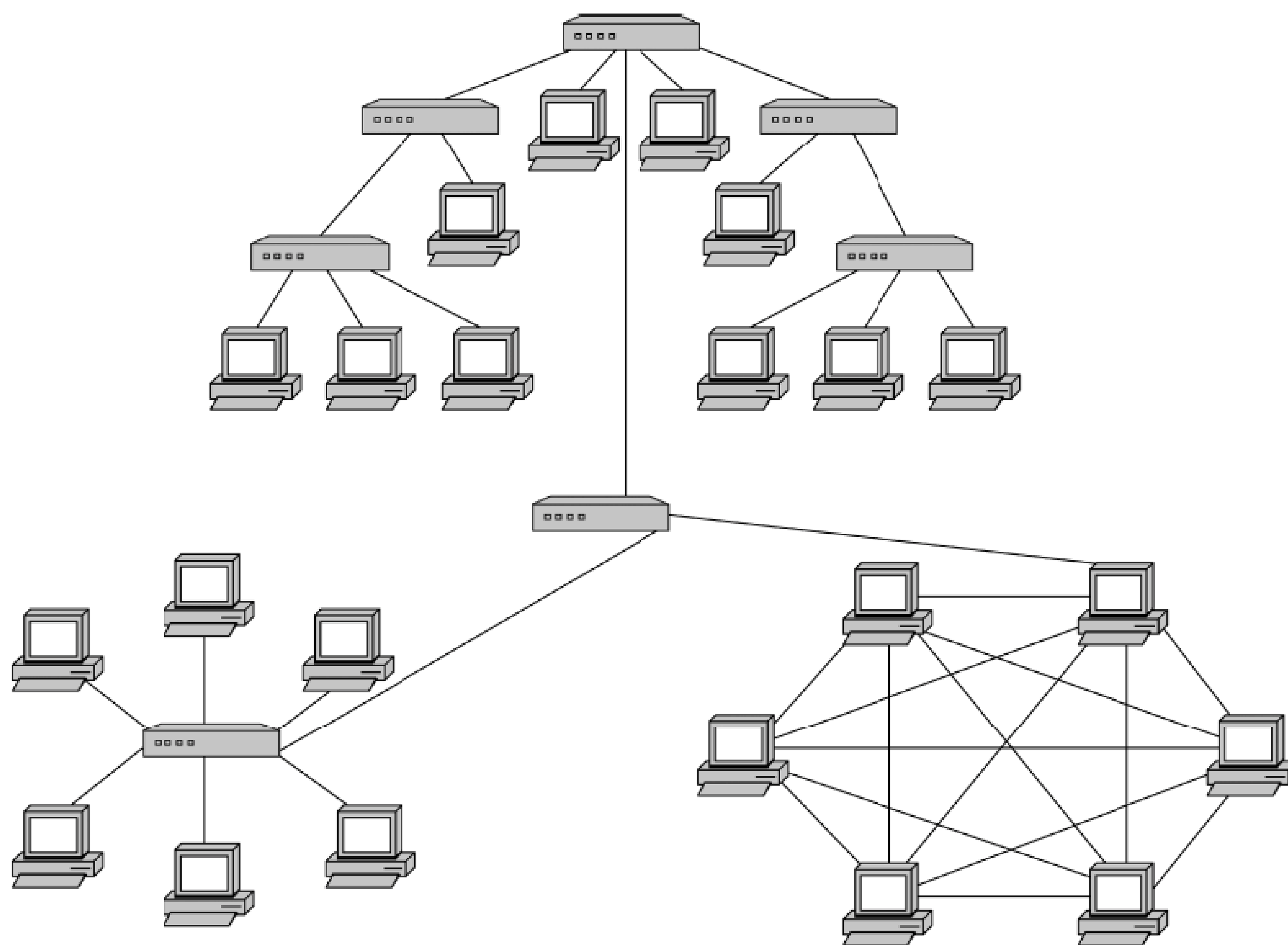


图 1.5　星网树混合拓扑结构

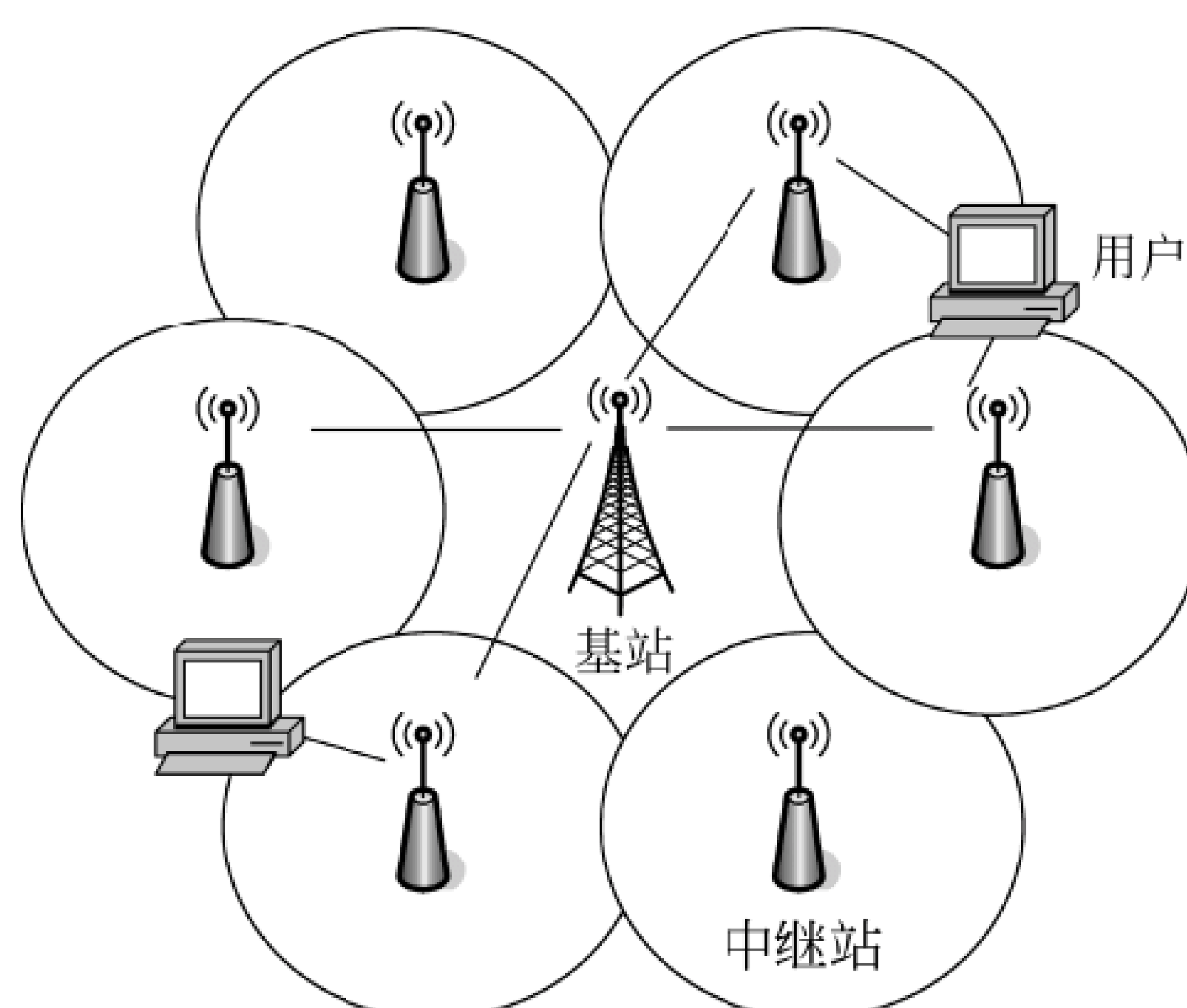


图 1.6　蜂巢拓扑结构

1.2　信号与信道

通信子网是计算机网络的基础。数据信号通过通信系统发送、传输和接收。图 1.7 为通信系统的基本模型。

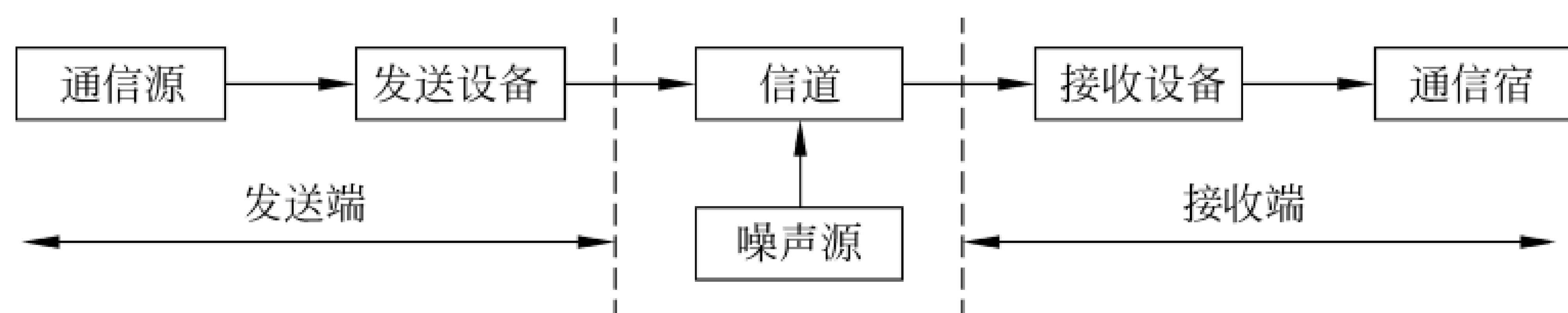


图 1.7　通信系统的基本模型

其中：

信源（source/sender）是数据信号的发生地；信宿（receiver）是数据信号接收地。在计算机网络中，信源与信宿主要是计算机，此外还有交换机、路由器等。

信道（channel）是数据信号的传输通道。信道传输数据信号时，往往会有噪声（noise）加入到信号中。

信道对于信号上的传输是有限制的。为了将数据信号可靠地在信道中传输，常常要在发送端用发送设备进行某种转换，而后在接收端进行逆转换。

1.2.1 数据信号分析

1. 信号的时域表示法

时域表示法就是把信号的幅值表示成时间函数。用时域表示法表示信号时，可以显示出信号幅值随时间变化的规律。图 1.8 为三种不同波形的信号。

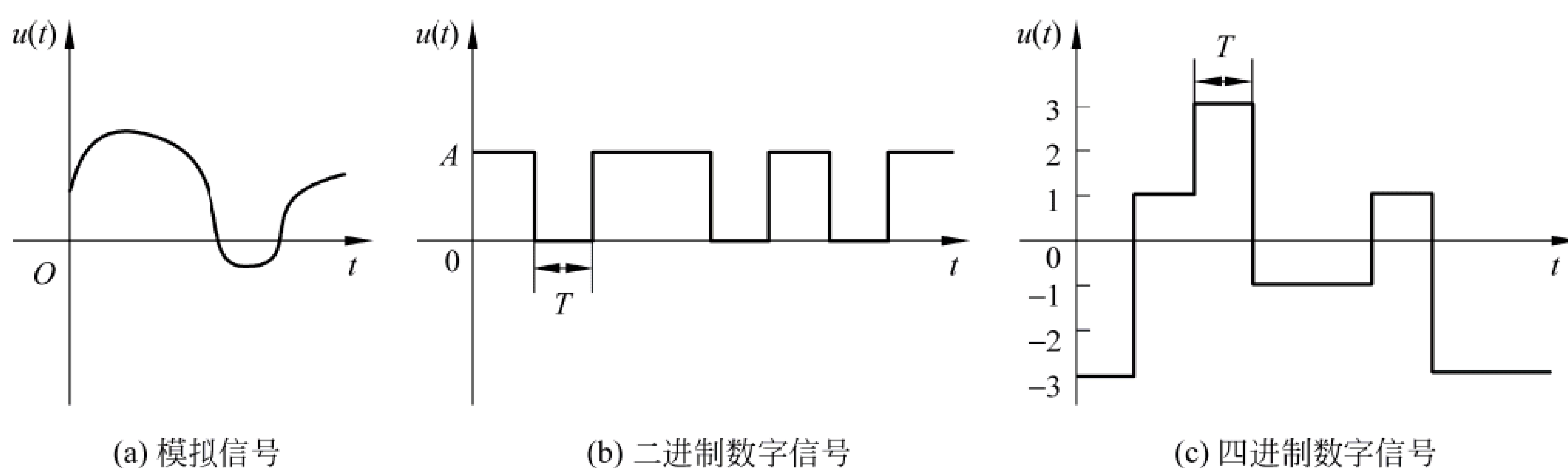


图 1.8 模拟信号与数字信号

模拟信号的时域特点是幅值连续，即在一定的时间区间内幅值可以取无限多个值，如图 1.8(a)所示。数字信号的时域特点是幅值不连续，即幅值只能取有限个值，如图 1.8（b）只能在 0、A 之中取值，图 1.8（c）只能在（3，1，−1，−3）4 个值之中取值。

典型的模拟信号是正弦波信号，频率、幅值和相位是正弦波的 3 个属性。

2. 信号的频谱表示法

1）信号的傅里叶分析

频谱表示法是把信号的幅值表示成频率的函数，以表明不同的谐波分量对信号的影响。这是基于傅里叶（Jean Baptiste Josepu Fourier,1768—1830）分析的一种方法：任何满足狄里赫利（Direchlet）条件的、频率为 f 的周期函数 $u(t)$都可以用一个直流分量和以其频率 f 为基频的各次谐波（三角函数）的线性组合表示，即

$$u(t)=\frac{1}{2}C+\sum_{n=1}^{\infty}a_n\sin(2\pi nft)+\sum_{n=1}^{\infty}b_n\cos(2\pi nft)$$

式中，C 是常数，a_n、b_n 是第 n 次谐波的幅值，$n=1$ 的分量波称为基波。

根据傅里叶分析，可以得到一个周期信号的谐波组成。一个信号的频率范围称为该信号的绝对带宽。在现实中，许多信号具有无限带宽，即它的傅里叶分析结果是无穷级数之和。不过，信号的大部分能量都集中在某一段频带之中，这个频带称为该信号的有效带宽，简称带宽。

用频谱表示方法，可以看出一种信号的频率范围——带宽，以及每一个频率分量的信号能量的大小。同一信号的时域表示与频谱表示之间有一定的关系。图 1.9 为 5 种不同信号时域表示与频谱表示的对应图。它表明，越接近正弦波，信号的带宽就越小，对信道的质量要求就越低；而越接近数字信号，信号的带宽就越宽，对信道的质量要求就越高。

2）影响信号谐波成分的因素

（1）谐波成分与信号形状有关。如图 1.9 所示为三种不同波形的信号所包含的谐波情况。

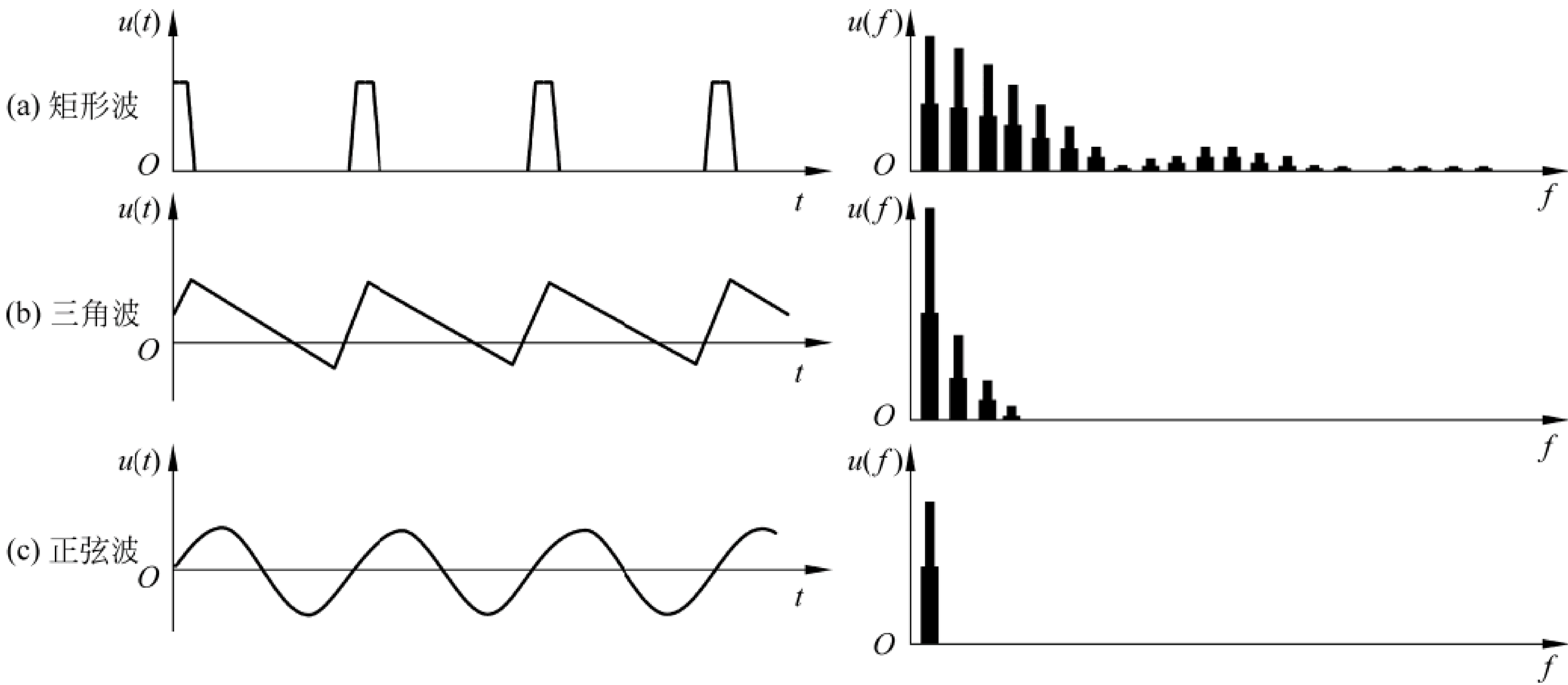


图 1.9　不同形状信号的时域表示与频谱表示

（2）数字信号中谐波的组成与数字信号的周期有关，也与脉冲宽度有关。通常，信号的周期越长，各谱线之间的间隔越小，如图 1.10（a）与（b）所示；信号脉冲越窄，其各谱线的零点频率越高，谐波分量越多，信号所占用带宽就越宽，如图 1.10（b）与（c）所示。这两个参数可以综合为一个参数：占空比，即脉冲宽度在周期中的比例。占空比越小，信号带宽越大。

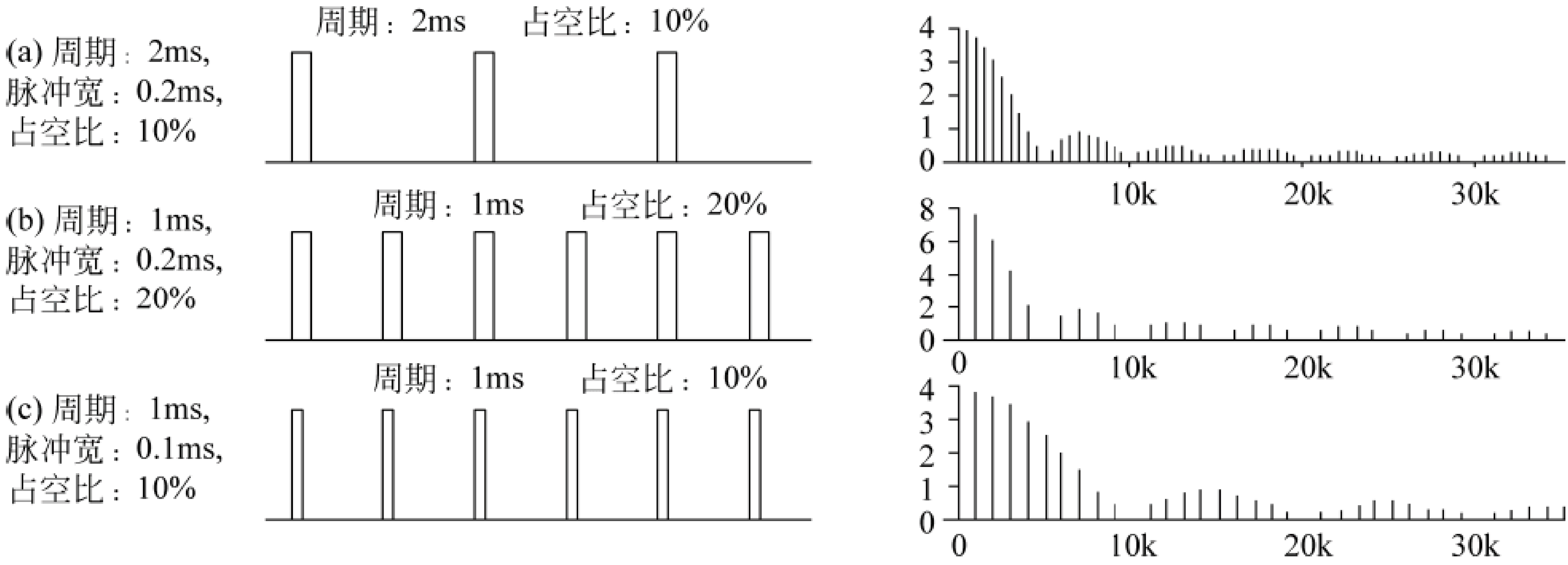


图 1.10　数字信号的周期越长，各谱线之间的间隔越小

1.2.2　信道及其类型

信道是信号的传输通路。信道可以有多种分类方法。下面介绍几种最基本的类

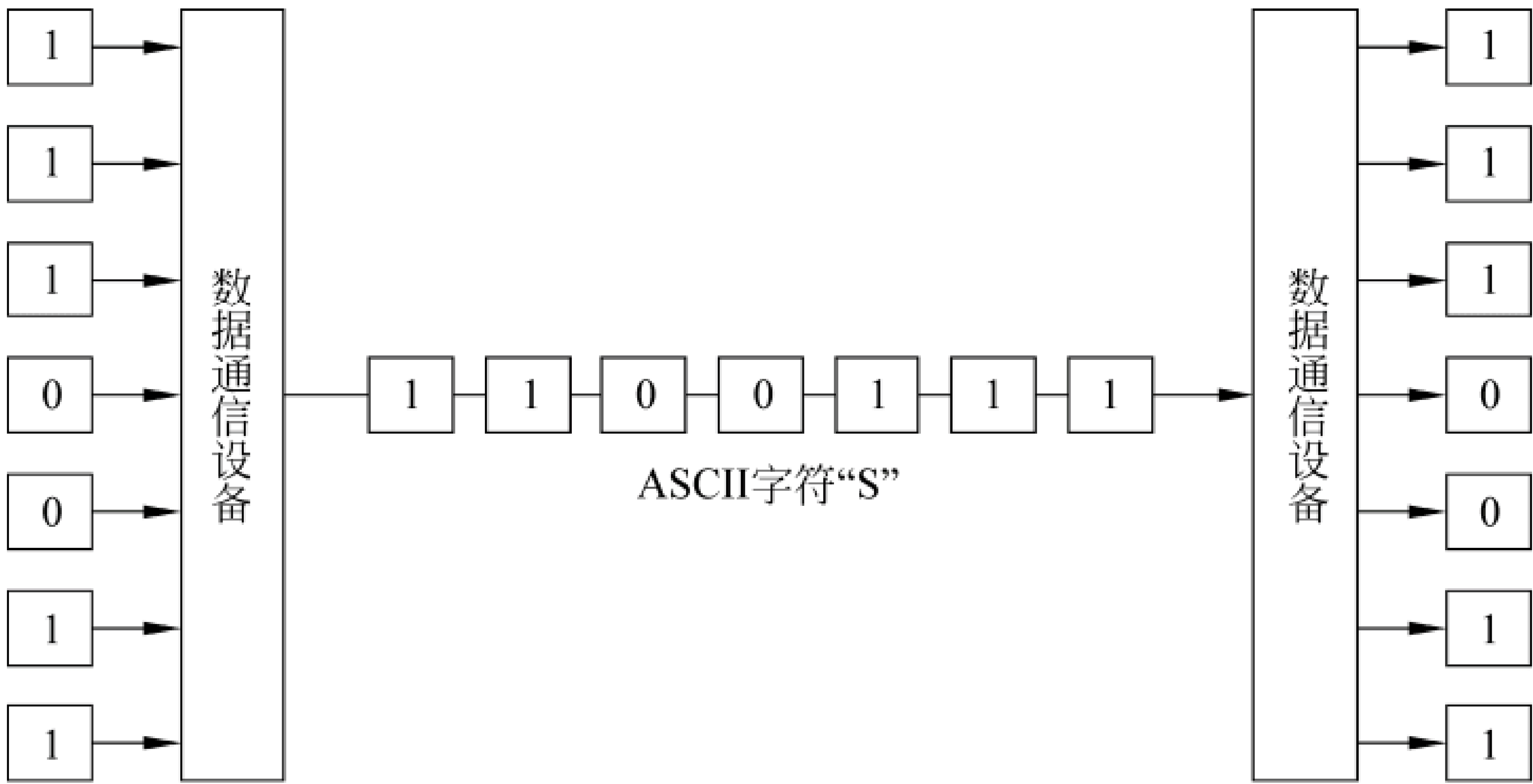
型。

1. 按照一次所能传输的数字信号的位数分类

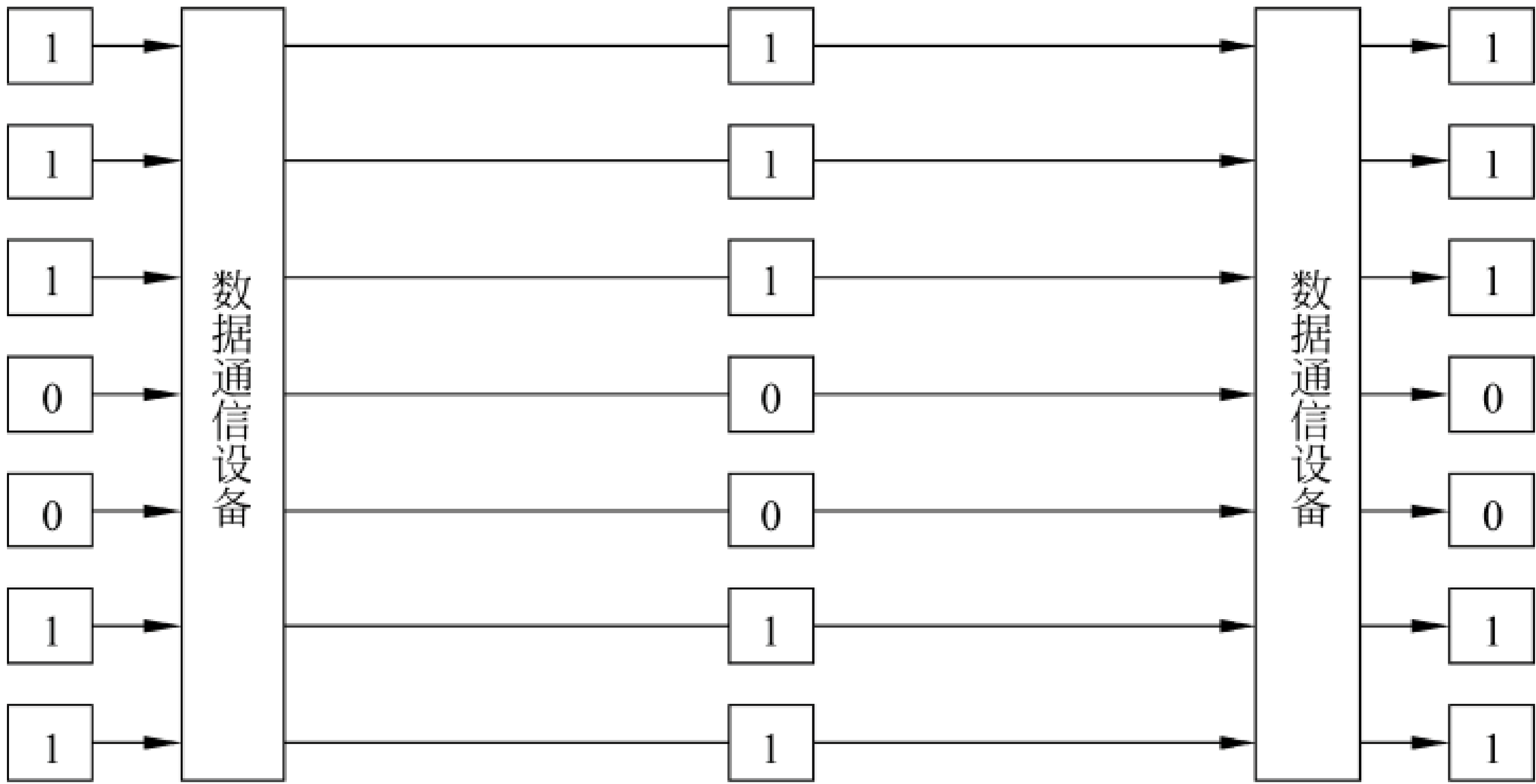
在数字信道中，按照一次所能传输的单位，可以分为串行通信信道和并行通信信道。

1）串行通信信道

串行信道每次只能传送一个二进制位码，即多位数据（如字节）必须一位一位地依次传输，每一位数据占据一个固定时间片。如图 1.11（a）所示，假定发送端向接收端要发送字母“S”（字母 S 的 ASCII 码值为 1100111），则传输时由低位到高位逐位传送“1110011”二进制比特序列。



(a) 串行通信



(b) 并行通信

图 1.11　串行信道与并行信道

2）并行通信信道

并行信道收发双方之间有相应多条传输线路，可以一次性传输若干个比特的数据，如图 1.11（b）所示，为了同时传输字符“S”，收发双方需用 7 条传输线分别传输其一个二进制位的 0 或 1。

2．按照传输的方向性分类

在数据传输中，按照交互传输的方向性，信道可以分为如下 4 种方式。

1）单工信道

如图 1.12（a）所示，单工是指数据的传输总是单向的，只能由一方将数据传输给另一方，如无线电广播，其信号只能由电台到用户终端（收音机）传输。只适宜单工传输信号的信道称为单工信道。

2）半双工信道

如图 1.12（b）所示，半双工是指数据可以在收、发双方间相互传递，但任何一个时间点上只能是单向的，如对讲机，听的时候不能说，反之说的时候不能听。只适宜半双工传输信号的信道称为半双工信道。

3）全双工信道

如图 1.12（c）所示，全双工是指数据可以在收、发双方间同时相互传递，如手机、程控电话，听的时候也能同时说，说的时候也能同时听，边说边听，毫无影响。适宜双工传输信号的信道称为双工信道。

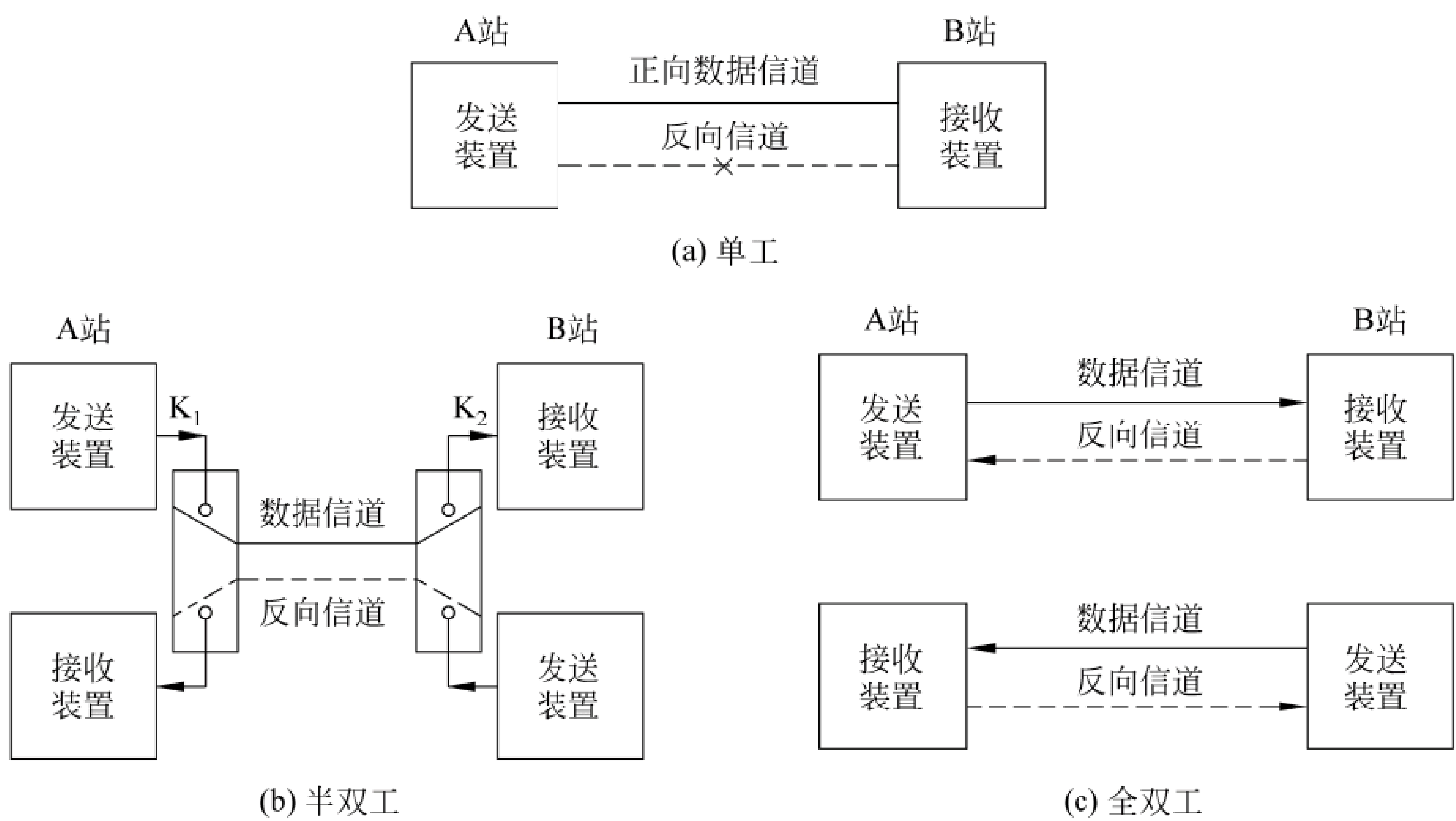


图 1.12　单工、半双工和全双工通信

4）全双工/半双工自适应

设备具有智能性，可以根据具体环境，自动变换传输模式。

3．按照传输介质的物理特征分类

根据传输介质是否有形，信道可以分为有线信道和无线信道。有线信道包括双绞线、同轴电缆、光纤等有形传输介质。无线信道包括红外线、无线电波、微波、可见光、卫星通信等以波的形式进行数据传输的信道。

4．按照允许传输的信号类型分类

根据允许传输的信号类型，信道可分为模拟信道和数字信道。

模拟信道只允许输模拟信号，如电话线。数字信道允许传输的是数字信号。要让数字信号在模拟信道中传输，需要进行 A/D 转换。

5．物理信道和逻辑信道

物理信道是指计算机网络结点间的物理连接，它由传输介质及有关通信设备组成。逻辑信道是在物理连接的基础上，由结点的对等层通过协议建立的、能够传递相应数据单元的连接。显然，用于传送数据的通信信道一定是在物理信道基础上建立起来的逻辑信道，而且在同一物理信道上可以提供多条逻辑信道，就像一条铁道线上，可以允许多个车次的列车通行一样，而每一逻辑信道上只允许一路信号通过。

1.2.3 信道的技术指标

一个计算机网络的技术指标很多是由信道的技术指标决定的。

1．信道的带宽（bandwidth）和容量

1）模拟通信系统中的带宽——通频带

最早的电子通信采用模拟技术。在模拟通信中，不同的传输介质允许的电磁波频率范围也不同。图 1.13 给出了各种通信介质的适用频率范围，其单位是赫兹（Hz）、千赫（kHz）和兆赫（MHz）等。这个频率范围称为带宽或通频带。对于一个具体的通信系统来说，根据所采用的技术，会在其所用介质的频带中处于某一段的位置。

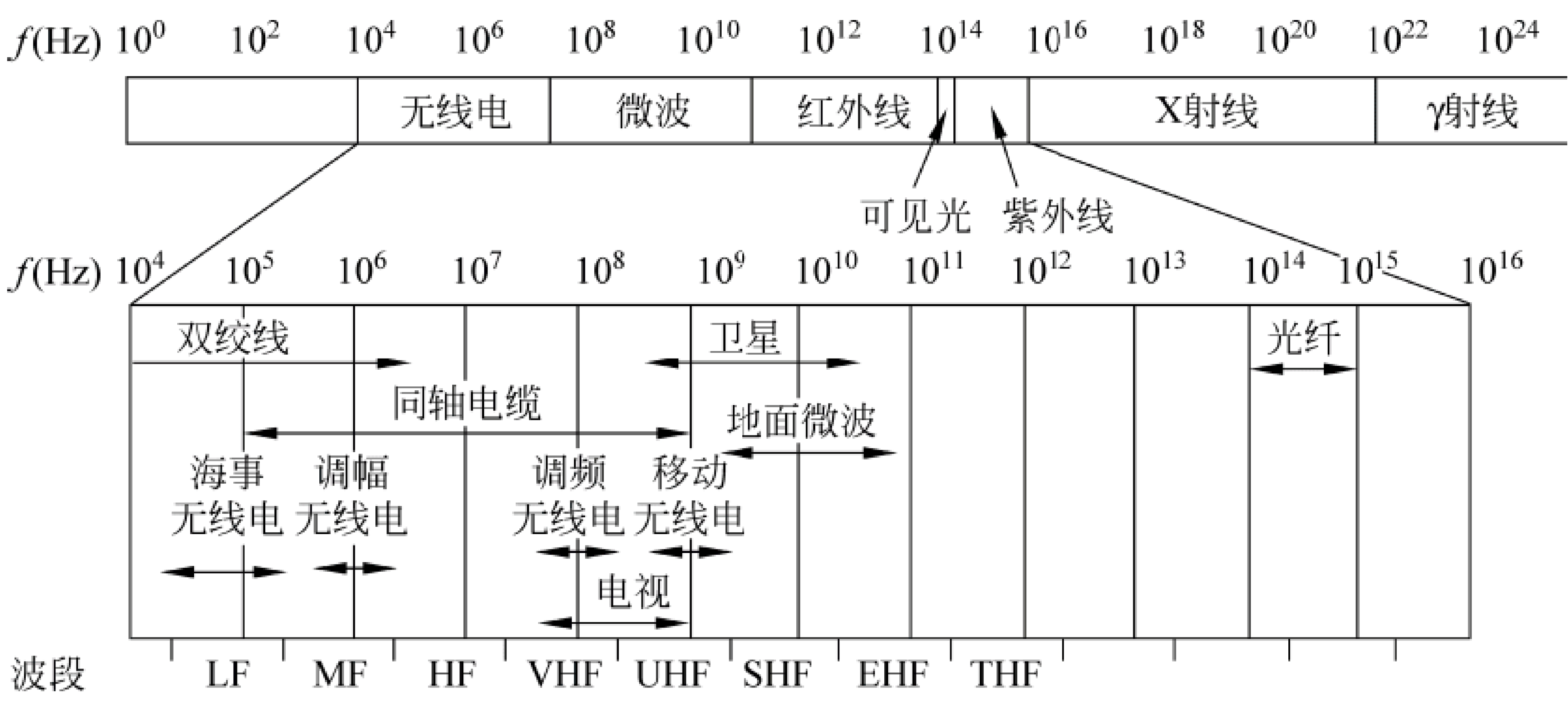


图 1.13　不同传输介质的频率范围

2）数字传输通信系统中的带宽——信道容量

在数字通信系统中，带宽是指在单位时间内网络中能够通过的最高数据量，即最高传输速率。单位为 b/s（bps）、kb/s、Mb/s、Gb/s、Tb/s 等。这里，量词 k、M、G 和 T 的含义采用通信领域中的约定。这些量词在通信领域和计算机领域中的含义区别见表 1.1。

信道容量是信道所能传输数据的理论值。在实际应用中，网络的实际传输速率往往达不到信道容量，如 56kbps 的调制解调器在一般的线路上的实际传输速率只能达到 33.6kbps 甚至更小。因此，信道容量往往是一个极限参数。

表 1.1　常用量词在计算机领域与通信领域的含义

使用领域	k/K（千）	M（兆）	G（吉）	T（太）	应用举例
通信领域	$1k=10^3$	10^6	10^9	10^{12}	带宽
计算机领域	$1K=2^{10}=1024$	2^{20}=1 048 576	2^{30}=1 073 741 824	2^{40}	存储容量、信息量大小

2. 信噪比与误码率

在电路和通信系统中，有用信号以外的所有干扰信号总称为噪声。任何非理想信道都会遭受干扰而形成噪声。这种能量场对于通信的影响可以大致分为两类：

（1）线性失真（linear distortion）是由于信道中存在阻抗，使不同频率的分量产生不同的衰减和时延（相移），引起信号波形变化。这种失真可以在发送端或接收端安装均衡器消除。均衡器可以根据信道的传输特性，对不同频率的分量进行调整，使它们传送到接收端后总的衰减时延基本相同。

（2）非线性失真（nonlinear distortion）由噪声产生。按照来源，噪声可以分为内部噪声和外部噪声。内部噪声包括（因为信号传输使信道的物理参数发生变化而产生的）热噪声和散弹噪声等。外部噪声包括自然噪声（如雷电、宇宙噪声）和人为噪声（其他电器设备以及传输信号的干扰）。

噪声对于信道的影响用信号的平均功率与噪声的平均功率之比评价，称为信噪比（Signal-To-Noise Ratio，SNR）。信噪比高，说明噪声在信号中占的比例小。

如图 1.14 所示，在数字传输系统中，噪声叠加在信号上，会引起某些位的信号在接收端错误地被接收。这称为误码。引起误码的另一个因素就是信道带宽所引起的信号失真。传输系统的带宽低，信号的失真就严重，信噪比就低，误码率也高。因此，在数字传输系统中用误码率来评价信道的传输质量。

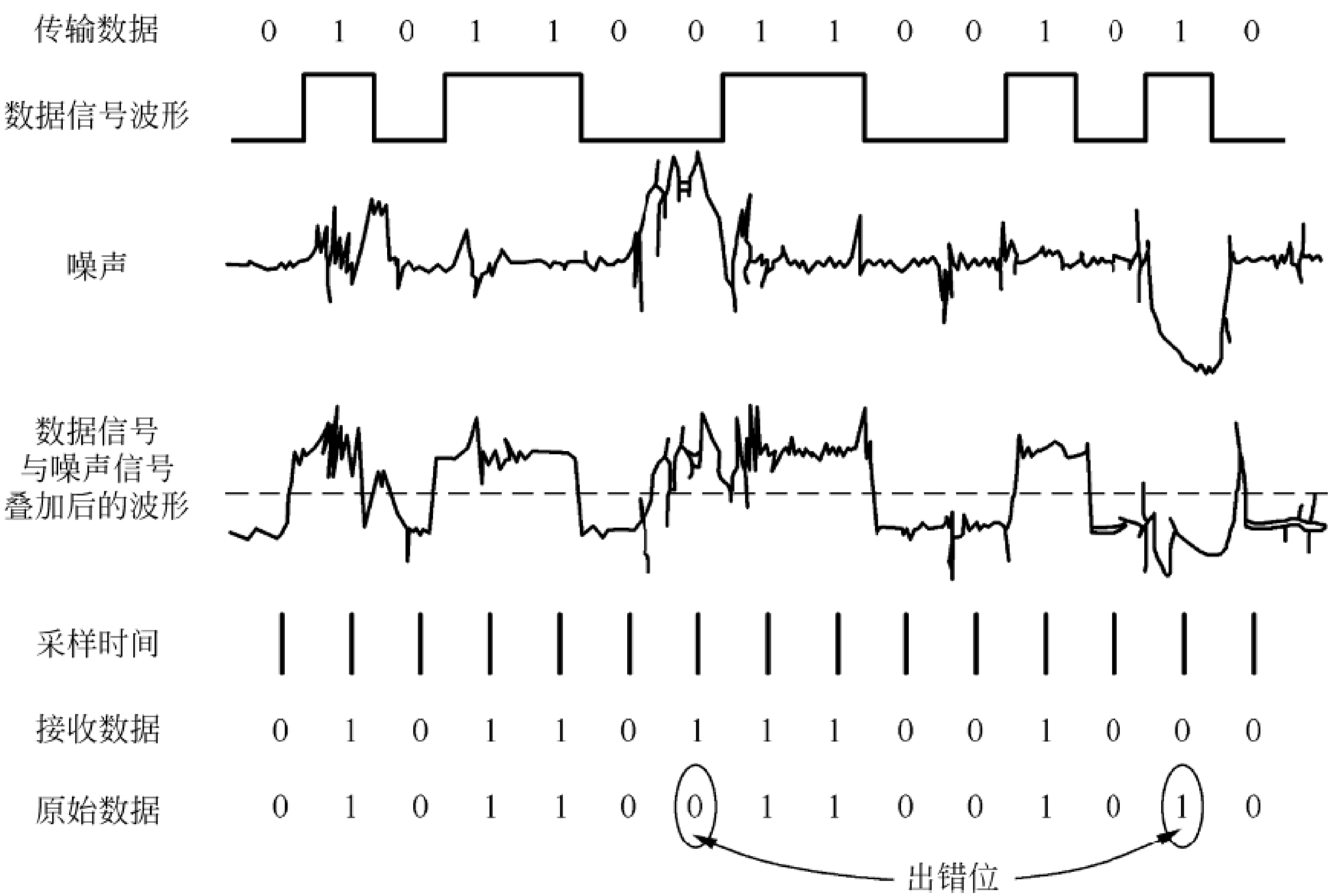


图 1.14　噪声引起的误码

误码率是数据通信系统在正常工作情况下的传输可靠性指标，指信道传输信号的出错率，用下面的公式表示：

$$P_e = \frac{N_e}{N}$$

式中，N 为数据传输的总位数，N_e 为数据传输过程中出错的位数。通常计算机网络要求误码率低于 10^{-6}，即每传送 1 兆位数据，不能出现多于一个错误。

3. 时延

时延（delay）是指数据由信源传输到信宿过程中所耗费的时间，其单位是秒（s）、毫秒（ms）、微秒（μs）等。数据在通信时，一般要经过 4 个过程：处理（主要指数据在缓冲区中排队等待）、发送（将要传送数据从计算机送到传输介质上）、传播和接收。这 4 个过程都需要一定的时间，形成通信中的 4 种时延。图 1.15 为 4 种时延产生的示意图。

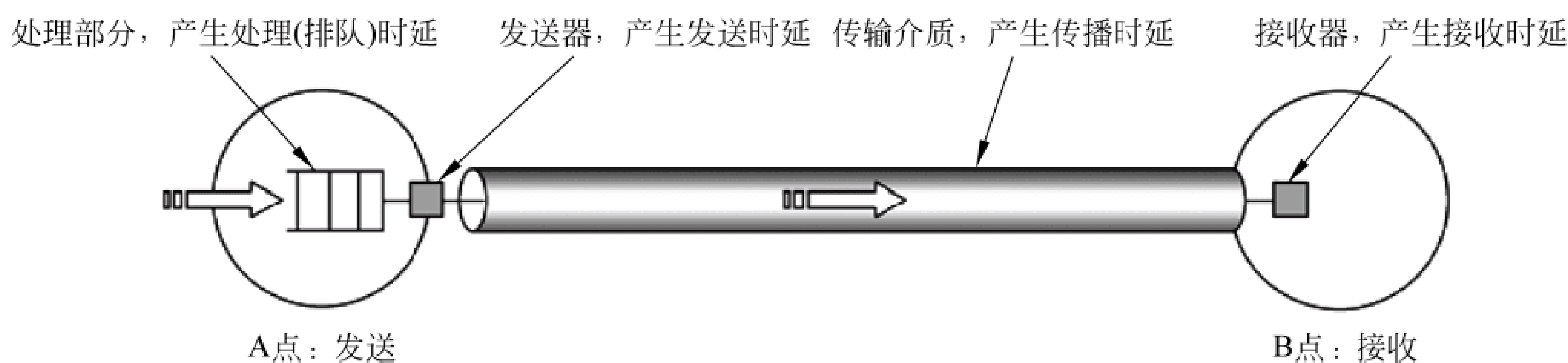


图 1.15　通信中时延的产生

可以看出：

传输总时延 ＝ 处理时延 ＋ 发送时延 ＋ 传播时延 ＋ 接收时延

并非传播时延低的信道，带宽一定高。例如，光波在光纤中的传播速率为 205Mm/s，而电流在 5 类铜线中的传导速率为 321Mm/s。但是，为什么常说“光纤的数据传输率比铜线高”呢？原因就是数据在光纤信道上的发送速率高。

下面进一步分析发送时延与传播时延之间的关系。假如只传输 1 个字节的数据，用光纤传输 100km 的距离，则传播时延为 $100\times10^3/(2.0\times10^5) = 0.5$s。若在带宽为 1Mb/s 的链路中传输，发送时延为 8×10^{-6}s；不考虑排队处理时延，传输总时延为 0.500 008s。若在 100Mb/s 的链路中传输，发送时延为 8×10^{-4}s，不考虑排队处理时延，传输总时延为 0.5008s。显然，传播时延几乎没有影响总时延——总传送时间。

此外，由于排队往往具有随机性，不是通信系统自己固有的特征，一般不能将此作为影响带宽的因素。因此，在如图 1.15 所示的 4 个因素中，发送/接收速率是与总时延关系最密切的因素，也是与信道带宽关系最密切的因素。例如一个长度为 200MB（这里，1M 为 2^{20}=1 048 576，1B=8bit）的数据块，要在 1Mb/s（这里，1M=10^6）的链路中传输，则发送时延不能超过 $200\times1\ 048\ 576\times8/10^6$=1677.8s，即必须在不超过近半小时的时间内把这个数据块发送完毕。但是若在带宽为 100Mb/s 的链路上传输，则必须在 16.7s 内将这些数据发送完毕。

注意，使用带宽 2Mb/s 的接入网络，并不等于每秒钟最高可以下载 2Mb 的数据。因为，2Mb=2000kb=250kB，即数据传输时奇偶校验位用了 250kb，所以每秒钟实际传输的数据量

最大为 2000kb–250kb = 1750kb=1.75Mb。

1.2.4 数字信号的模拟传输

1. 基带信号、基带传输与频带传输

在通信领域中，信源发出的原始信号被称为基带信号（baseband signal）。它们可以是模拟信号，也可以是数字信号。图 1.16 为一张声波频谱分析图，可以看出其频带环境。考虑更一般的情况，可以认为基带信号具有如下两个特征：

- 低频分量。一般认为也包含了直流分量。
- 高频特征。一般认为频率可以是无穷大。

通常也把具有以上两个特征的信号称为基带信号。

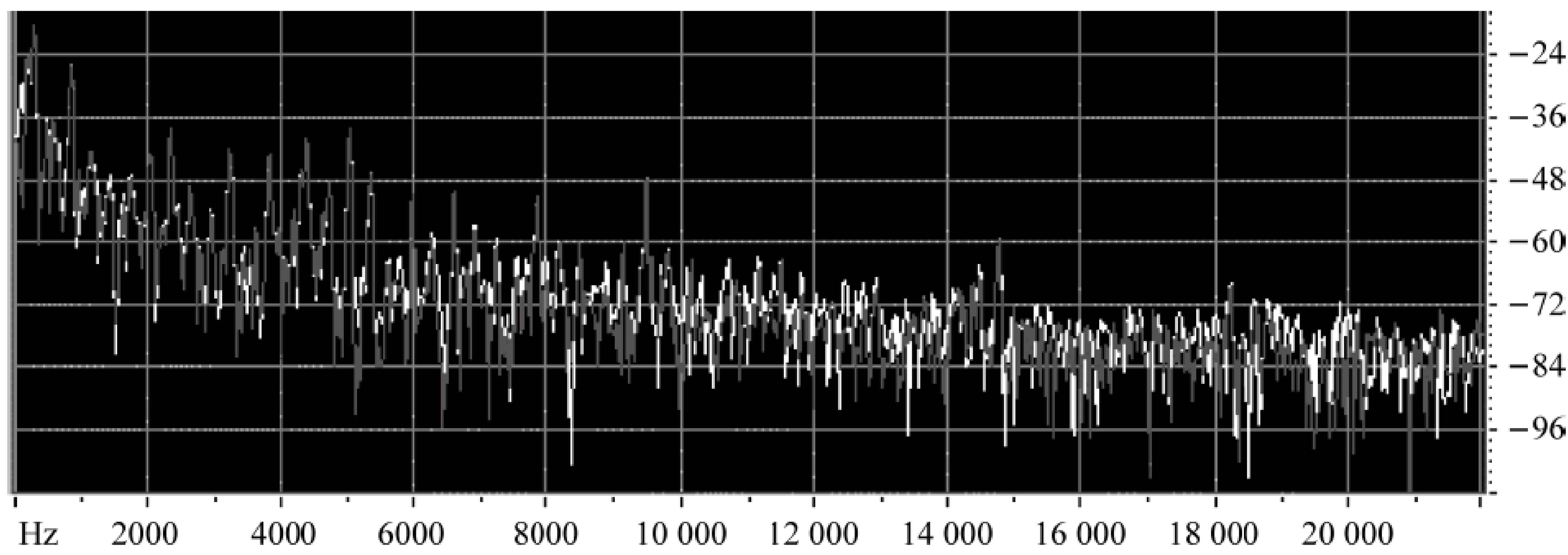


图 1.16 一张声波频谱分析图

基带传输指可以直接进行基带信号的传输。基带传输一般用于计算机内部的并行传输以及距离不远的计算机网络传输中。因为距离近，信号的畸变很小，可以控制在工程允许的范围内，基带传输不适合远距离传输。为了进行远距离传输，必须将基带信号变换成带宽较窄的频带信号。这种传输称为频带传输。

2. 信号的调制与解调

将不适合传输的信号变换为适合在信道中传输的信号称为调制（modulation）。经过调制的频带信号传送到信宿端后，要还原成原来的基带信号。这个过程称为解调（demodulate）。由于通信多是双向的，所以在实际应用中调制与解调两部分功能要做在一个设备——调制解调器（Modem）中。图 1.17 为一个简单的使用 Modem 的通信模型。

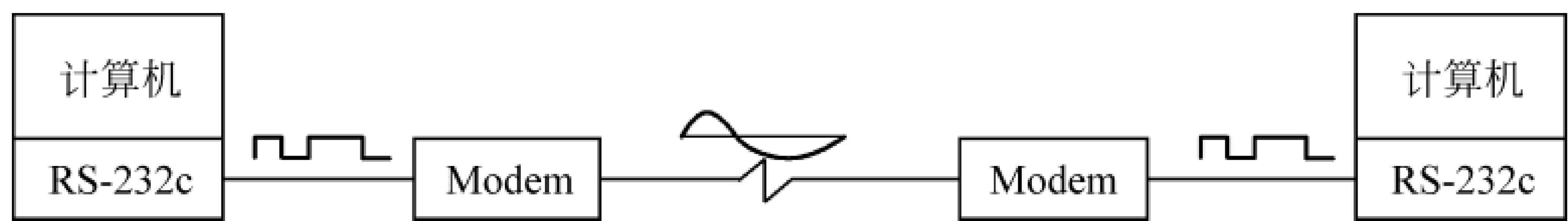


图 1.17 用 Modem 进行计算机通信

进行信号调制基本方法是把带宽很宽的基带信号变换为带宽很窄的信号——称之为频带信号或通带信号（belt pass signal）。这样的调制称为频带调制。实际上，频带调制就是频带搬移——把一个基带信号搬移另外一个通频频带上，或者说是用频带信号承载基带信号。所以这种调制也称为载波。

频带的选择，因传输介质而异。例如无线传输的频带位于高频区。此外，频带的带宽应当很窄。最理想，也是最常用的方法是移动键控调制，就是把数字信号变换为正弦信号，或者说用正弦信号载波数字信号。

设用于载波数字信号的正弦波为

$$u(t) = u_m \sin(\omega t + \phi_0)$$

在这个式子中，除时间 t 外，还有 3 个参数：振幅 u_m、角频率 ω 和相位 ϕ_0。因此，可以采用调幅、调频、调相 3 种移动键控技术来进行数字数据的模拟调制，分别称为幅移键控（amplitude-shift keying，ASK）、频移键控（Frequency-Shift Keying，FSK）和相移键控（Phase-Shift Keying，PSK），如图 1.18 所示。

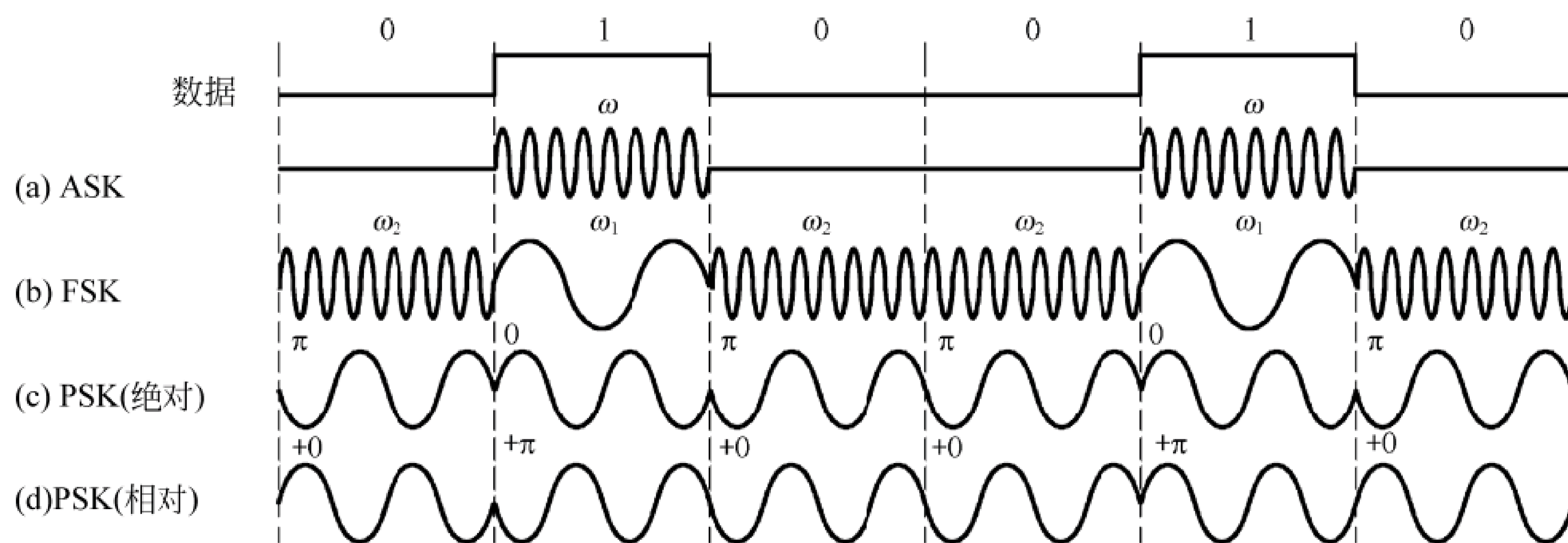


图 1.18　数字/模拟信号调制

1）幅移键控（ASK）

在 ASK 方式中，用不同幅值的正弦载波信号来分别表示数字 1 和 0。例如，用某一幅值的正弦载波信号表示数字 1，用零幅值（无载波信号）表示数字 0。ASK 的技术简单、实现容易，但抗干扰能力差。

2）频移键控（FSK）

在 FSK 方式中，用不同角频率的正弦载波信号来分别表示数字 1 和 0。FSK 的技术简单、实现容易、抗干扰能力强，是目前最常用的方法。

3）相移键控（PSK）

在 PSK 方式中，用不同初相位的正弦载波信号来分别表示数字 1 和 0。它的抗干扰能力强，但实现技术复杂。具体的实现方法有：绝对调相（用相位的绝对值表示数字 1 和 0）、相对调相（用相位的相对偏移值表示数字 1 和 0）和多相调相（用不同的相位值表示 0 和 1 码组合，如用相位相差 π/2 的相位值分别表示 00、01、10、11）。

3．模拟信号的数字编码——脉冲编码调制技术

模拟数据的数字编码是将连续的信号波形用有限个离散（不连续）的值近似代替的过程。简单地说，就是将模拟信号用数字信号近似地代替，其中最常见的方法是脉冲编码调制（Pulse Code Modulation，PCM）技术，简称脉码调制。PCM 的基本步骤如下。

- 采样：即将原波形的时间坐标离散化，得到一系列的样本值。
- 量化：对采样得到的样本值按量级分级并取整。

- 编码：将分级并取整的样本值转换为二进制码。

如图 1.19 所示为 PCM 过程的一个实例。

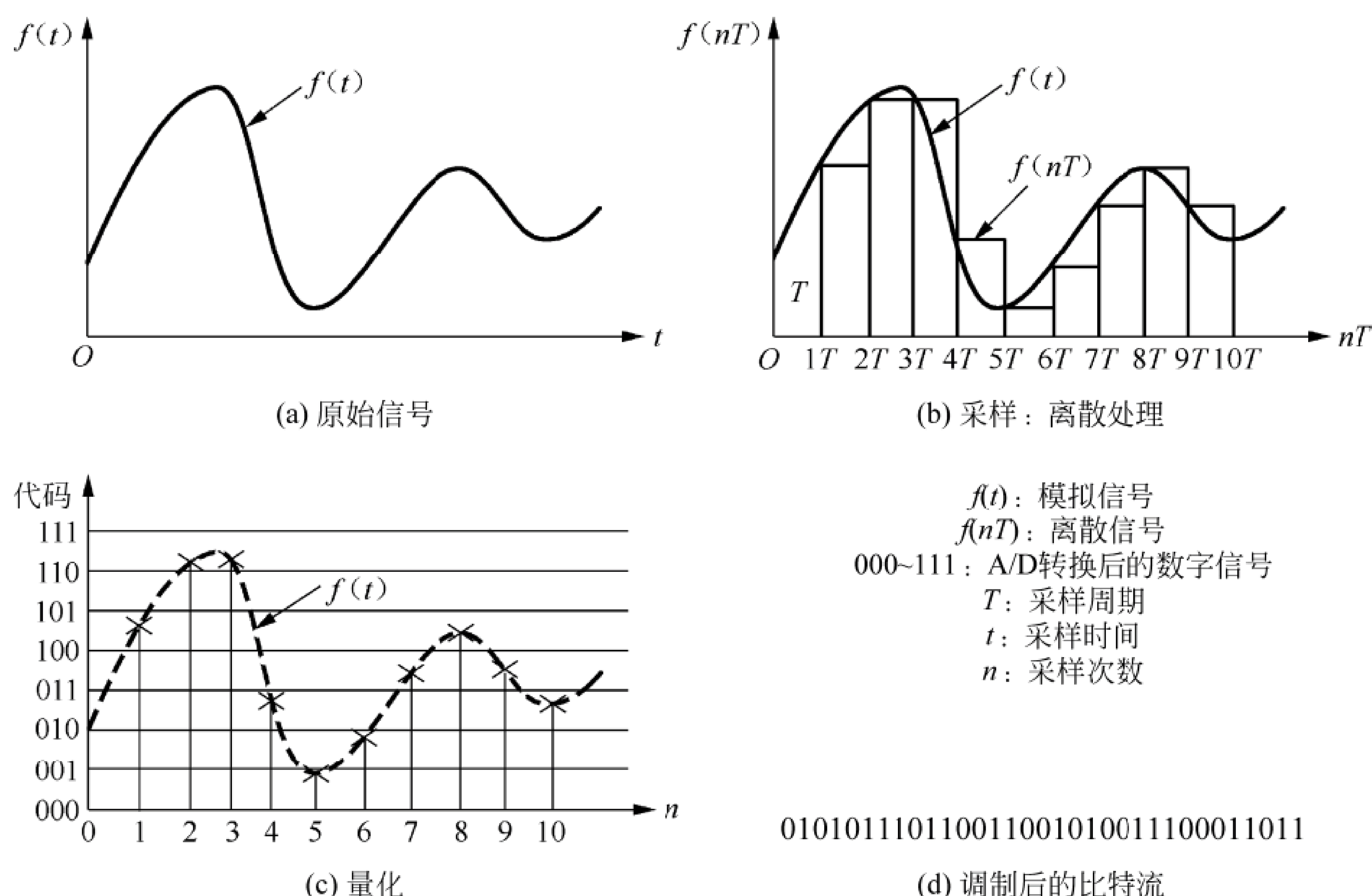


图 1.19 PCM 过程实例

数字化的质量取决于下列技术参数。

1）采样频率

采样频率，即一秒钟内的采样次数，它反映了采样点之间的间隔大小。间隔越小，丢失的信息越少，采样后的图形越细腻和逼真。根据奈奎斯特采样定律，只要采样频率高于信号最高频率的两倍，就可以从采样准确地重现原始信号的波形。

2）测量精度

测量精度是样本在垂直方向的精度，是样本的量化等级，它通过对波形垂直方向的等分而实现。由于数字化最终要用二进制数表示，所以常用二进制数的位数表示样本的量化等级。若每个样本用 8 位二进制数表示，则共有 2^8=256 个量级；若每个样本用 16 位二进制数表示，则共有 2^{16}=65 536 个量级。量级越多，采样精度越高。

应当指出，采样频率和测量精度的提高都以存储容量和处理时间为代价。此外，当考虑通信双方的同步、信息保密、信息压缩等问题时，还要对这种基本编码进行一些变换。

1.2.5 数字信号的数字编码

数字信号的数字编码也称为基带调制，它与频带调制的区别是，不移动频带，仅做数字信号形状的变化，目的是改变信号的传输特性。基带调制的方法很多，目的是获取不同的数字信号传输特性，为此人们设计了多种编码方法。下面介绍几种具有代表性的编码。

1. 二元位编码

位编码是针对原始的 1 和 0 分别定义编码规则。二元是指在编码过程中使用的也是二

进制符号。它们是基本的数字编码形式，也分为不同类型。图 1.20 所示为 5 种基本的二元位编码。

1）*单极性码和双极性码*

（1）图 1.20 中的（a）和（c）表示的是两种单极性码，即电流只有一个极性（方向）。或者说，可以只在表示 1 时发出电流，也可以只在表示 0 时发出电流，因此它们具有如下特点：

- 只用一个电压值，能耗小，成本低。
- 具有较大直流分量，会导致信号失真与畸变，无法使用于交流耦合的线路和设备上。
- 抗噪性能差。
- 需要一端接地。

（2）图 1.20 中的（b）和（d）表示的是两种双极性码，它们的特征是表示 1 和 0 时分别发出不同方向的电流，即电流具有两个极性（方向）。这种编码的主要特点是：

- 直流分量比较小，在 0、1 出现概率相等时基本不含直流分量。
- 容易设置，比较稳定，抗干扰能力强。
- 可以在无接地的信道上传输。

2）*归零码和不归零码*

（1）图 1.20 中的（c）和（d）表示的是两种归零码（Return to Zero，RZ），它们的特征是每次进行 0-1 变换或 1-0 变换时，都要在零电压处停留一下。这实际上也算一种双相码。注意，在双极性归零码中，虽然使用了三个电平，但零电压只是中间停留，不是作为一个值存在，这种编码的主要特点是：

- 每个比特位都发生信号变换，可以直接提取同步信号。特别是采用双极性归零码，可以自同步，不需要特别定时信号。
- 占空比为 50%，脉冲宽度小，码元能量低，占用带宽多。

（2）图 1.21 中的（a）和（b）表示的是两种不归零码（Non-Return to Zero，NRZ），它们的特征是每次进行 0-1 变换和 1-0 变换都是直接的，不在无电流处停留。单极性归零码中的零电压只是一个值，而不是一个中间停留值。这种编码有如下特点：

- 其占空比为 100%，发送能量大，占用频带较窄，效率较高。
- 不能提取同步信号，有连续的 0 或连续的 1 时，接收端无法分辨每个比特的头、尾。

3）*差分码*

差分（different）码用每一码元的开始边界处有无变化来区别 0 和 1。

如图 1.20（e）所示为有跳变表示 1，无跳变表示 0，称为带号差分码。

如图 1.20（f）所示为有跳变表示 0，无跳变表示 1，称为空号差分码。

2. 二元块编码

块编码也称 *n*B*m*B 码，即将 *n* 位码转编为 *m* 位。即一组（*n* 位）原始二元信息在编码后都用另一组（*m* 位）二进制码来表示，并且 $m > n$。最简单的 *n*B*m*B 码是 1B2B 码。此外还有 3B4B 码、4B5B 码、5B6B 码、8B9B 码、8B10B 码和 17B18B 码等。下面以 1B2B 码和 4B5B 码为例进行简单介绍。

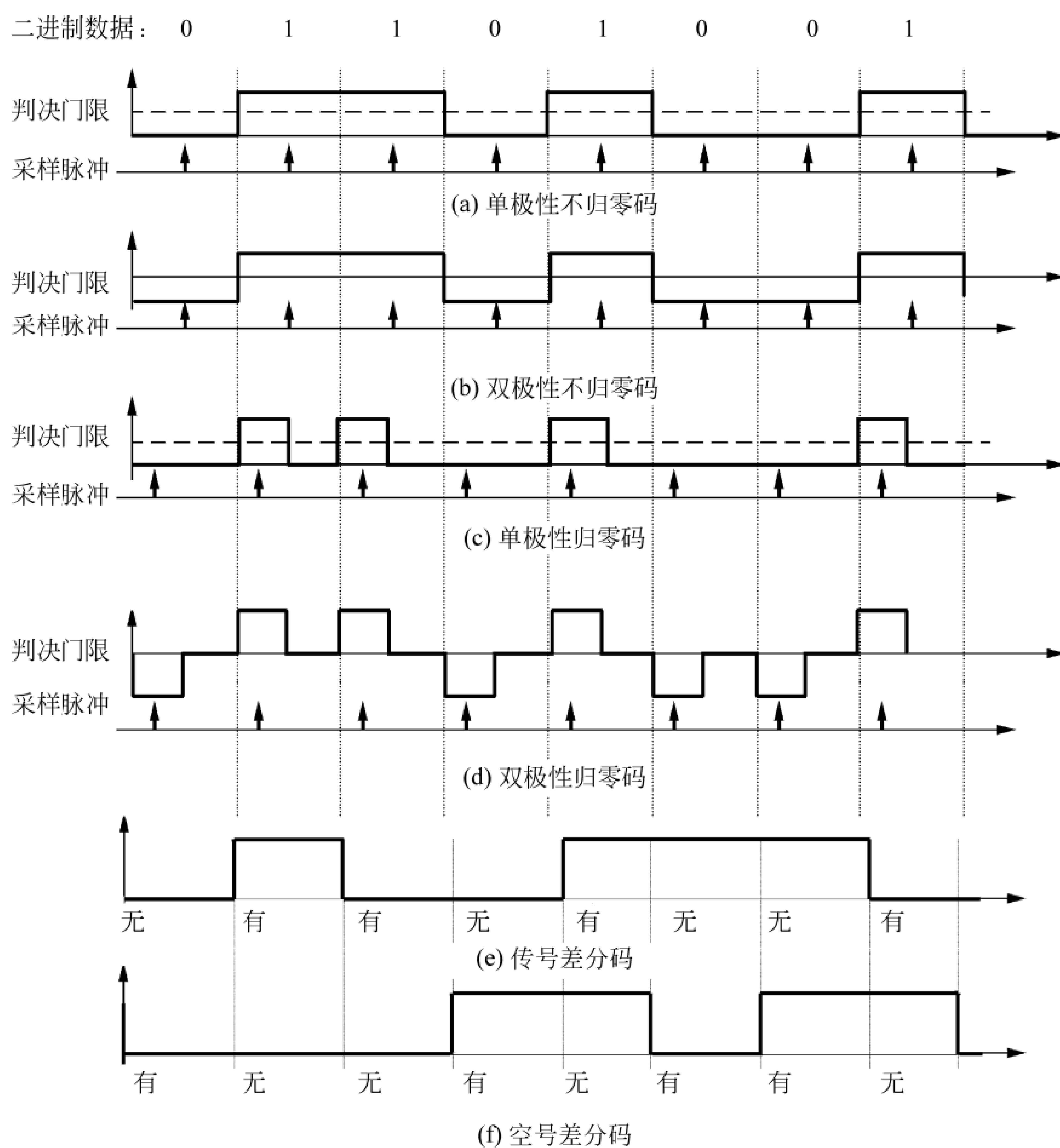


图 1.20　5 种基本的位编码方式

1）1B2B 码

1B2B 码的基本特点是用两位表示一个码。图 1.21 为几种常用的二元码。

（1）曼彻斯特（Manchester）码。

编码规则：0→01，1→10，如图 1.21（a）所示。

特点：

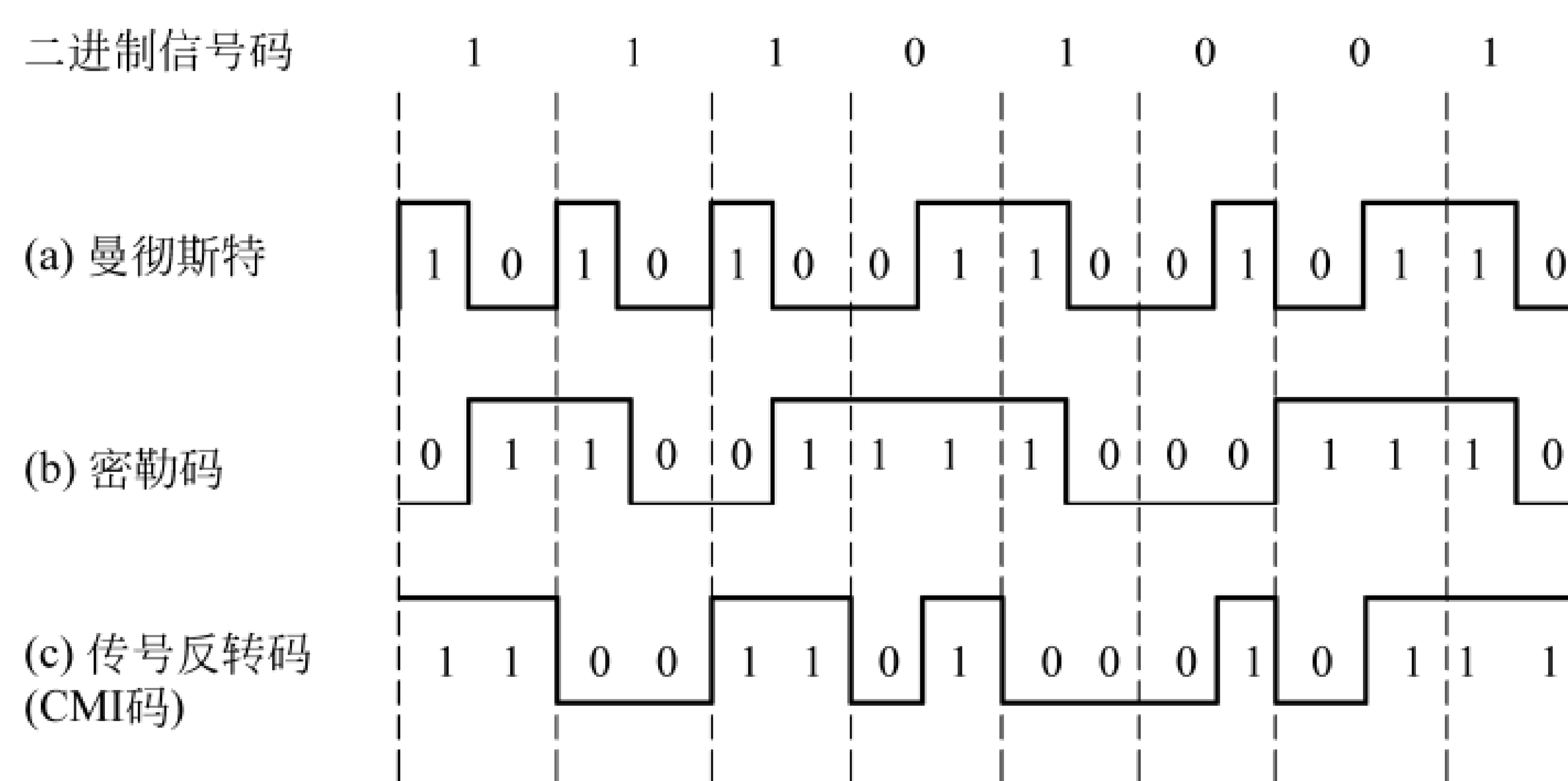


图 1.21　三种常用 1B2B 码

- 在每个比特周期的中间产生一个电平跃变，用正跃变表示为 0，用负跃变表示为 1，既能够提供足够的定时分量，又无直流漂移。
- 编码过程简单。
- 带宽是原始码的 2 倍。

（2）密勒（Miller）码。密勒码又称延迟调制码，它可以看成是双相码的一种变形。

编码规则如图 1.21（b）所示：

- 1→10 或 01，用码元持续时间中心点出现的跃变来表示，即用 10 或 01 表示。
- 0 码分两种情况处理：对于单个 0，在码元持续时间内不出现跃变，与相邻码元的边界处也不跃变；对于连 0，在两个 0 码的边界出现电平跃变，即 00 与 11 交替。

（3）CMI 码。CMI 码是传号反转码的简称。

编码规则：1 码交替用 11 和 00 表示；0 码用 01 表示，如图 1.21（c）所示。

这种码型有较多的电平跃变，因此含有丰富的定时信息。该码已被 CCITT 推荐为 PCM（脉冲编码调制）四次群的接口码型。在光缆传输系统中有时也用作线路传输码型。

2）4B5B 码

4B5B 编码是将欲发送的数据流每 4bit 作为一个组，然后按照表 1.2 所示的 4B5B 编码规则将其转换成相应 5bit 码。

表 1.2　4B5B 编码规则

十六进制数	4 位二进制数	4B5B 编码	十六进制数	4 位二进制数	4B5B 编码
0	0000	11110	8	1000	10010
1	0001	01001	9	1001	10011
2	0010	10100	A	1010	10110
3	0011	10101	B	1011	10111
4	0100	01010	C	1100	11010
5	0101	01011	D	1101	11011
6	0110	01110	E	1110	11100
7	0111	01111	F	1111	11101

5bit 码共有 32 种组合，但只采用其中的 16 种对应 4bit 码的 16 种，其他的 16 种或者未用或者用作控制码，以表示帧的开始和结束、光纤线路的状态（静止、空闲、暂停）等。

4B5B 码因其可以提取定时信号、低频分量小、效率高、同步迅速的优点和容易实现而被应用在 IEEE 802.9a 等以太网标准中。在同样的 20MHz 钟频下，利用 4B5B 编码可以在 10Mb/s 的 10Base-T 电缆上得到 16Mb/s 的带宽。

与 4B5B 码类似的 8B10B 码被应用在千兆以太网中。

3. 多元码

数字信息编码中使用多种符号时，称为多元码，也称多进制码。比如 *M* 元码的数字信

息中有 M 种符号，相应的必须有 M 种电平才能表示 M 元码。一般认为多元码是 $M > 2$ 的 M 元码。一个典型是应用在 100Base-T4 中的 8B6T 码。

所谓 8B6T，是指将 8b 映射为 6 个三进制位。如图 1.22 所示，其三进制的 3 个值为（+、0、–）。其编码规则如表 1.3 所示。

8B6T 100Base-T4 使用 4 对 3 类 UTP，采用的信号速度为 25MHz，每个周期发送 4b，就可获得所要求的 100Mb/s，还有一个 33.3Mb/s 的保留信道。

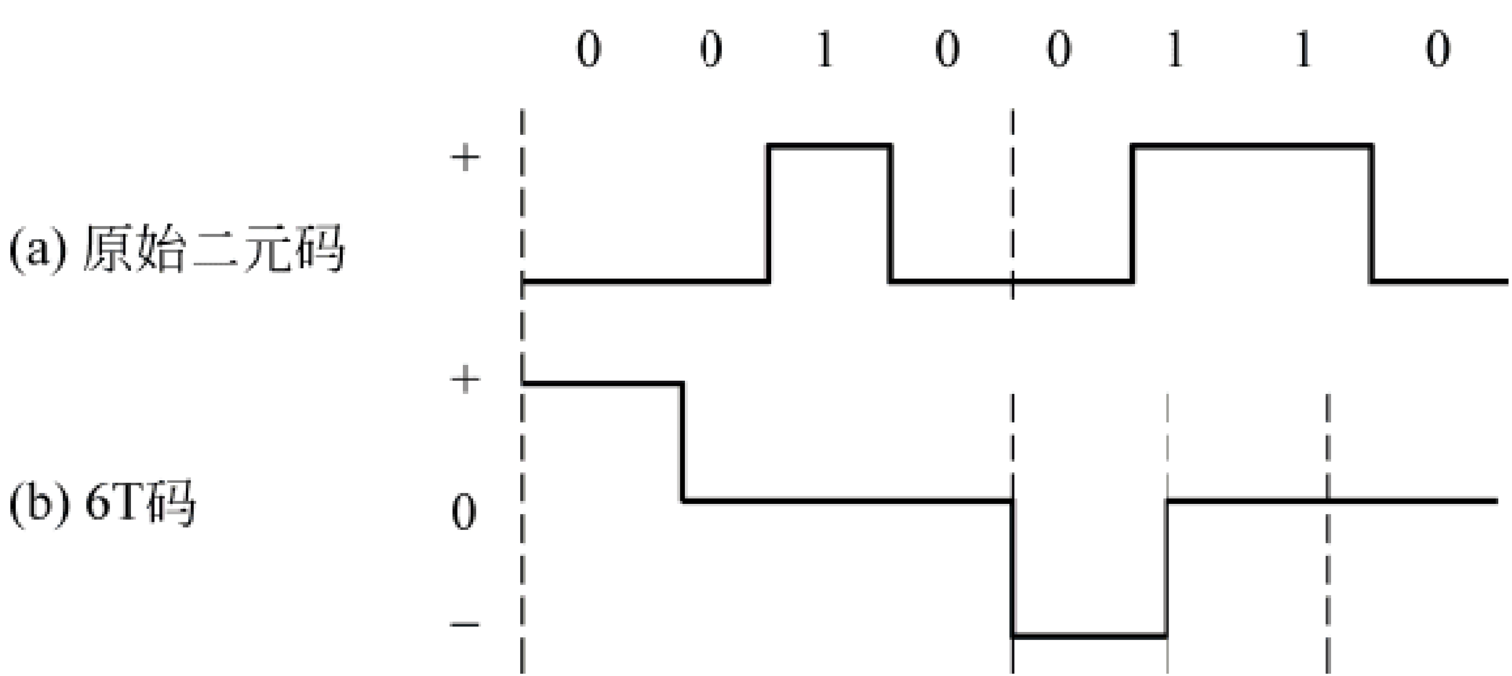


图 1.22　8B6T 编码

表 1.3　8B6T 编码规则

8 位数据	6T 码组	8 位数据	6T 码组	8 位数据	6T 码组	8 位数据	6T 码组
00000000	+-00+-	00001000	-+00+-	00010000	+0+--0	00011000	0+-0+-
00000001	0+-+-0	00001001	0-++-0	00010001	++0-0-	00011001	0+-0-+
00000010	+-0+-0	00001010	-+0+-0	00010010	+0+-0-	00011010	0+-++-
00000011	-0++-0	00001011	+0-+-0	00010011	0++-0-	00011011	0+-00+
00000100	-0+-0+-	00001100	+0-0+-	00010100	0++- -0	00011100	0-+00+
00000101	0+- -0+	00001101	0-+-0+	00010101	++00- -	00011101	0-+++-
00000110	+-0-0+	00001110	-+0-0+	00010110	+0+0- -	00011110	0-+0-+
00000111	-0+-0+	00001111	+0--0+	00010111	0++0- -	00011111	0-+0+-

1.2.6　多路复用技术

多路复用（MUX）源于拉丁语 multi（许多）和 plex（混合）。它指在一个物理信道上同时传送多路信号，或者说是把一个物理信道分成多个逻辑信道，以提高信道利用率。

1. 频分多路复用技术

频分多路复用（Frequency Division Multiplexing，FDM）是模拟传输中常用的一种多路复用技术。它把一个物理信道划分为多个逻辑信道，各个逻辑信道占用互不重叠的频带，相邻信道之间用“警戒频带”隔离，以便将不同路的信号调制（滤波）分别限制在不同的频带内，在接收端再用滤波器将它们分离，GSM 手机和无线广播就是两种典型的 FDM，虽同时传送多个频率信号，但可以分辨。如图 1.23 所示为将一个物理信道频分为 3 路进行复用的情形，每个逻辑信道分配 4000Hz 带宽，并只传送 3000Hz 左右的载波频带信号。

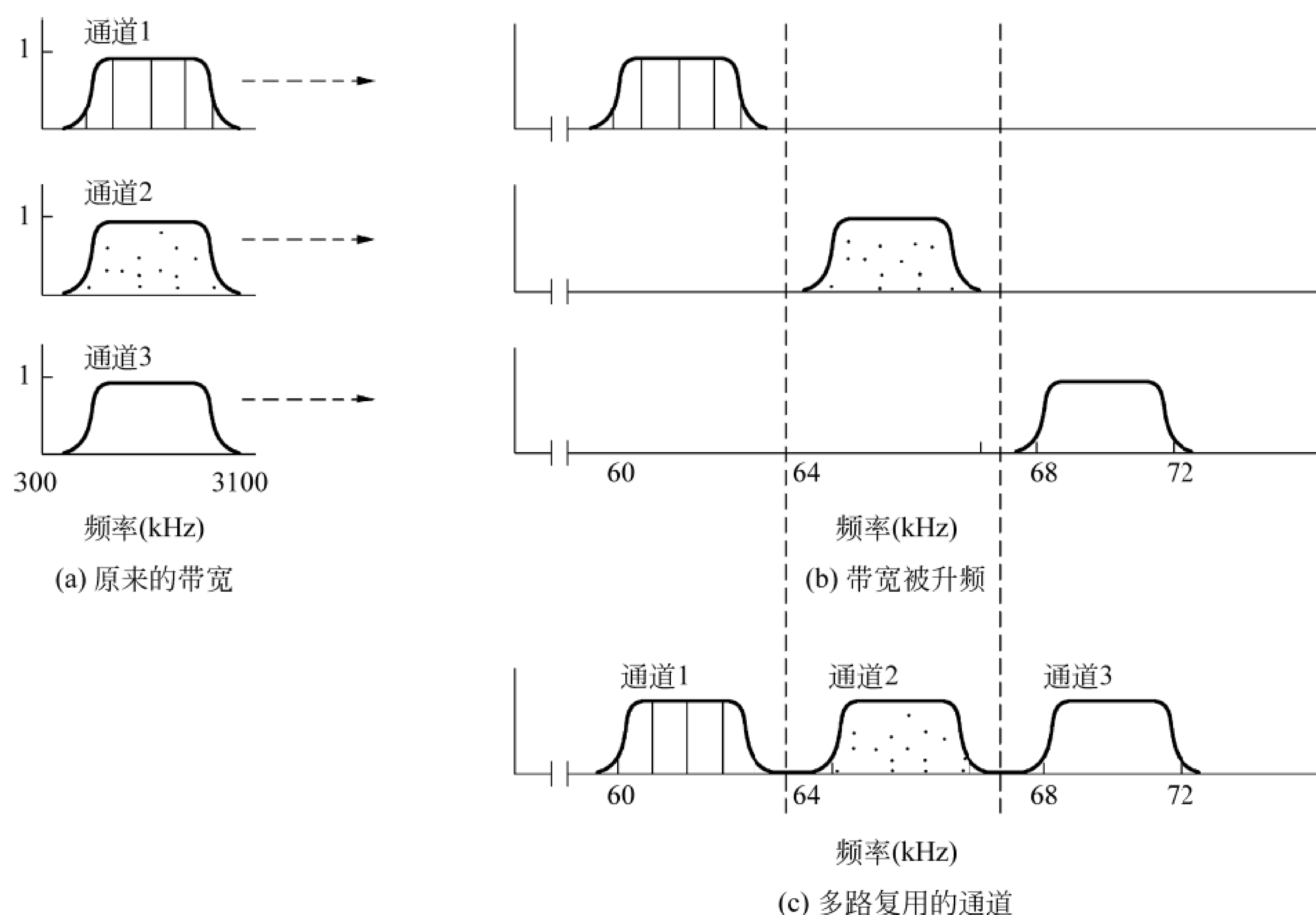


图 1.23　频分多路复用

2. 时分多路复用技术

与 FDM 的同时发送多路信号不同，时分多路复用（Time Division Multiplexing，TDM）是一种非同时发送的多路复用技术。如图 1.24 所示，它将一个传送周期划分为多个时隙，让多路信号分别在不同的时隙内传送，形成每一路信号在连续的传送周期内轮流发送的情形。

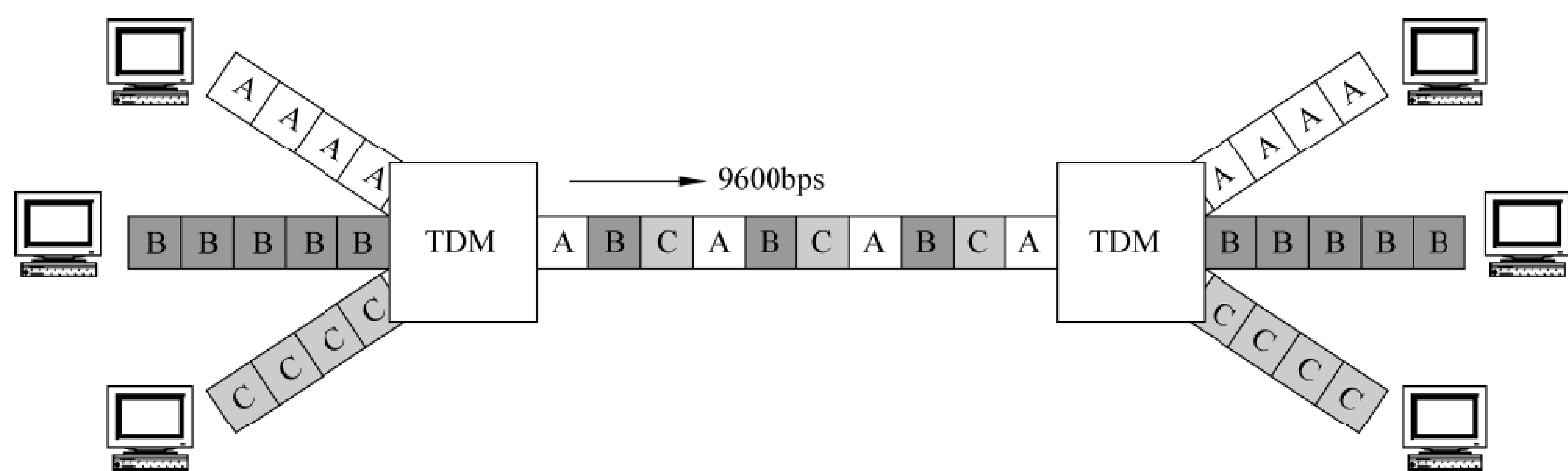


图 1.24　时分多路复用

数字信号的时分复用也称为复接，参与复用的信号称为支路信号，复用后的信号称为合路信号，从合路信号中将原来的支路信号分离出来称为分接。

通常，话音信号是用脉码调制来编码的。由于典型的电话通道是 4kHz，按照奈奎斯特定理，为了用数字信号精确地表示一个模拟信号，对话音模拟信号的采样频率至少要达到 8kHz。用一个 8 位字符来代表每个取样，则话音信号数字化的结果便是一个 8000×8（位）的数据流，数据传输速率为 64kbps。上述方法称为 PCM 复用。为了提高传输数码率，对 PCM 复用后的数字信号再进行时分复用，形成更多路的数字通信，这是目前广泛用来提高

通信容量的一种方法。

如图 1.25 所示为 ITU-T 推荐的数字速率等级和复接等级，它们都是基于传输速率 64 kbps（称为零次群）的数字信号的。两种等级不同之处在于，一类是用 TDM 技术将 24 路零次群复用到一条线路上，形成数据传输速率为 1.544Mbps 的一次群（称为 T1 次速率，主要在北美应用），并在此基础上形成其二次群、三次群、四次群等；另一类是用 TDM 技术将 30 路零次群复用到一条线路上，形成数据传输速率为 2.048Mbps 的一次群（称为 E1 次速率，主要在欧洲应用），并在此基础上形成其二次群、三次群、四次群等。

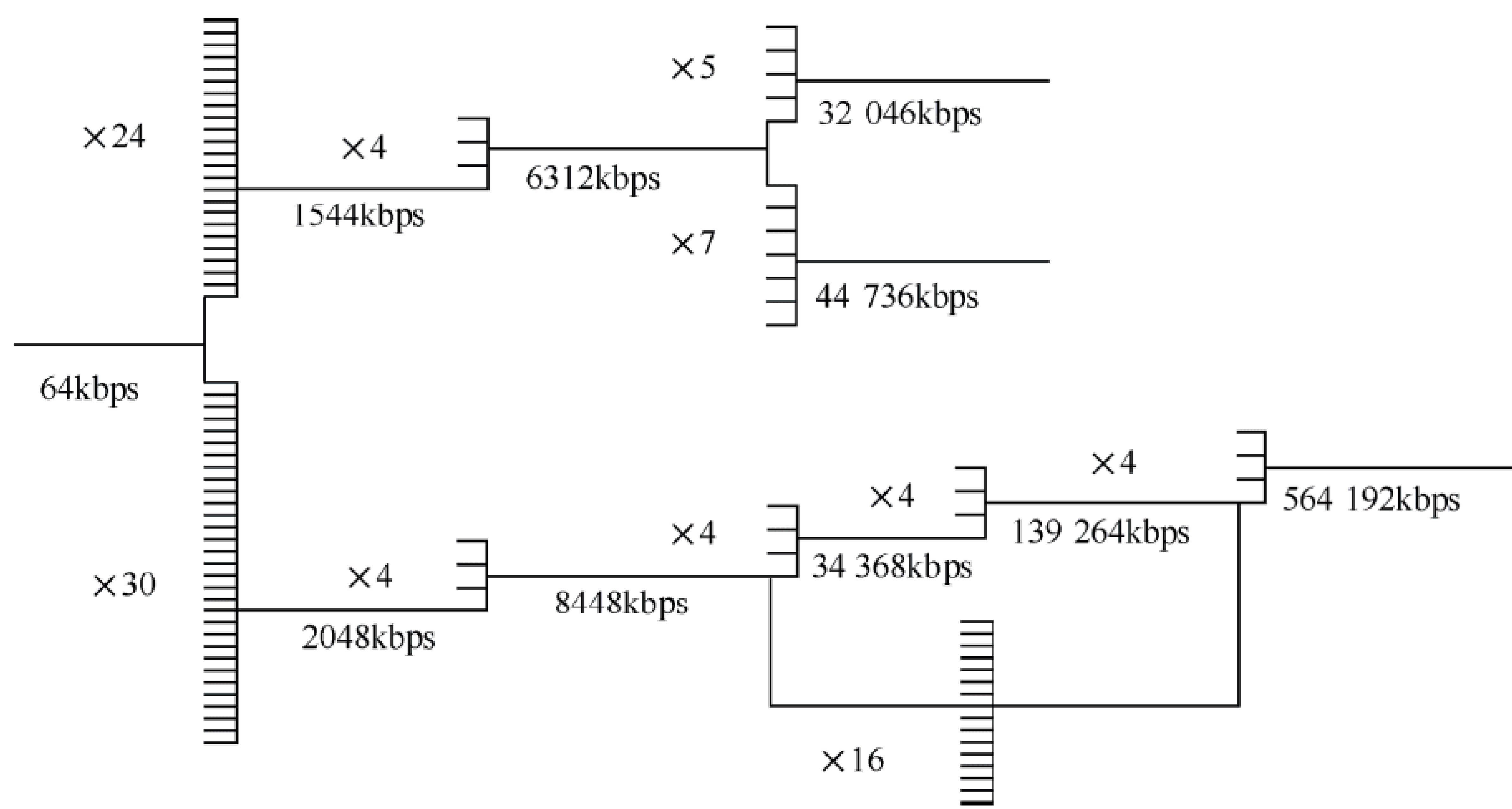


图 1.25　ITU-T 推荐的数字速率等级和复接等级

注意，时分多路复用只有在所传输的数据（通常称为报文——message）被分割成小块或段（通常称为分组——packet）时才有意义。假如一个报文需要传输 10 分钟，之后再传输另一个报文，这样的结果是各路传输都不可忍受。若把报文分组，情况就不同了。因为传输时延主要由发送时延、传播时延和接收时延三部分组成。当报文分组足够小时，传播时延将大大小于发送时延和接收时延之和。利用这个时间差可以在介质上进行其他路的数据传输。这就是时分多路复用的基本原理，也是划分时间片的基本依据。从另外一个方面看，提高发送和接收的速度是提高传输带宽的关键。但是，提高了发送和接收速度，就要求时间片划得更小，分组更小。

3. 光波分多路复用技术

光波分多路复用（Wavelength Division Multiplexing，WDM）技术是在一根光纤中能同时传输多个光波信号的技术。WDM 的基本原理如图 1.26 所示，它是在发送端将不同波长的光信号组合起来，复用到一根光纤上，在接收端又将组合的光信号分开（解复用），并送入不同的终端。

在 WDM 的基础上，1998 年研究成功了 DWDM，即密集波分多路复用技术，它可以处理传输速率高达 80Gbps 的业务，并将传输速率提高到了 800Gbps。目前，已经可以做到在一根光纤上传输 80 路以上的光载波信号。

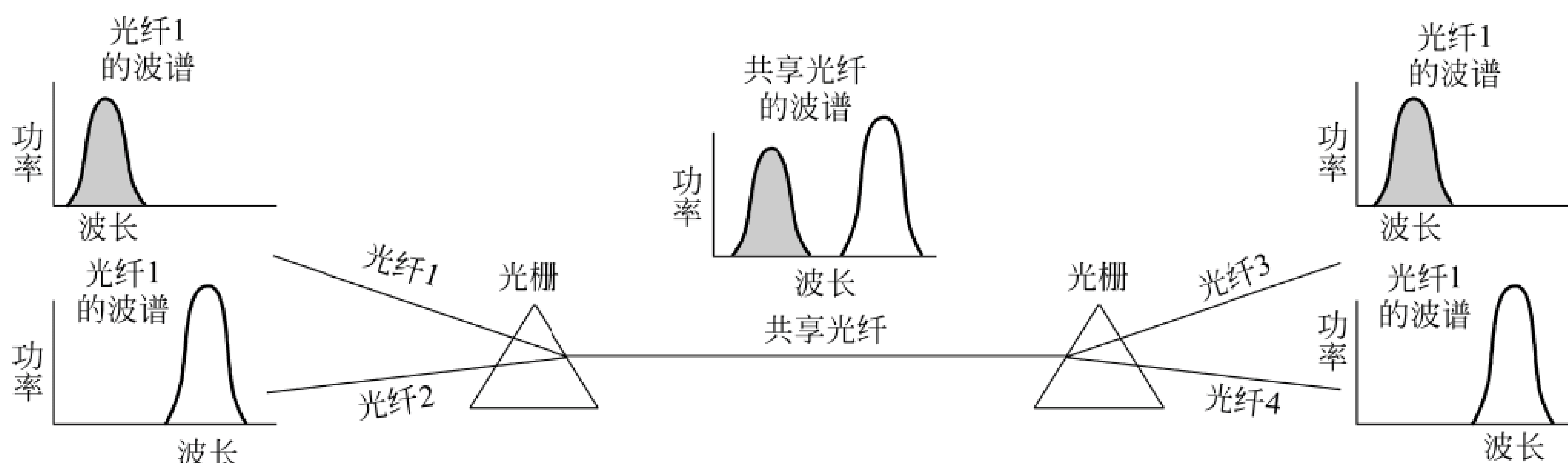


图 1.26　光波分多路复用单纤传输

4. 码分多路复用技术

码分多路复用（Code Division Multiplexing，CDM）是与码分多址（Code Division Multiple Access，CDMA）相联系的一项技术。

在 CDMA 传输时，要给每位用户分配一个 *m*（通常 *m* 取 64 或 128）比特序列，称为码片序列（chip sequence）或码片向量。不同的用户拥有不同的码片序列，好像他们具有不同的地址。

CDMA 按照下面的规则进行用户数据的发送：

- 发 1，发送该站的码片序列的原码；
- 发 0，发送该站的码片序列的反码。

如图 1.27 所示为一个发送用户码元比特流 1001 的例子。为了便于说明原理，假定 *m*=16，发送站是码片序列为 1110001101010010，其反码为 0001110010101101。于是，所发送的每一个用户比特都被扩展为 *m* 位的码片序列流，信号的频率带宽也被扩展了 *m* 倍。

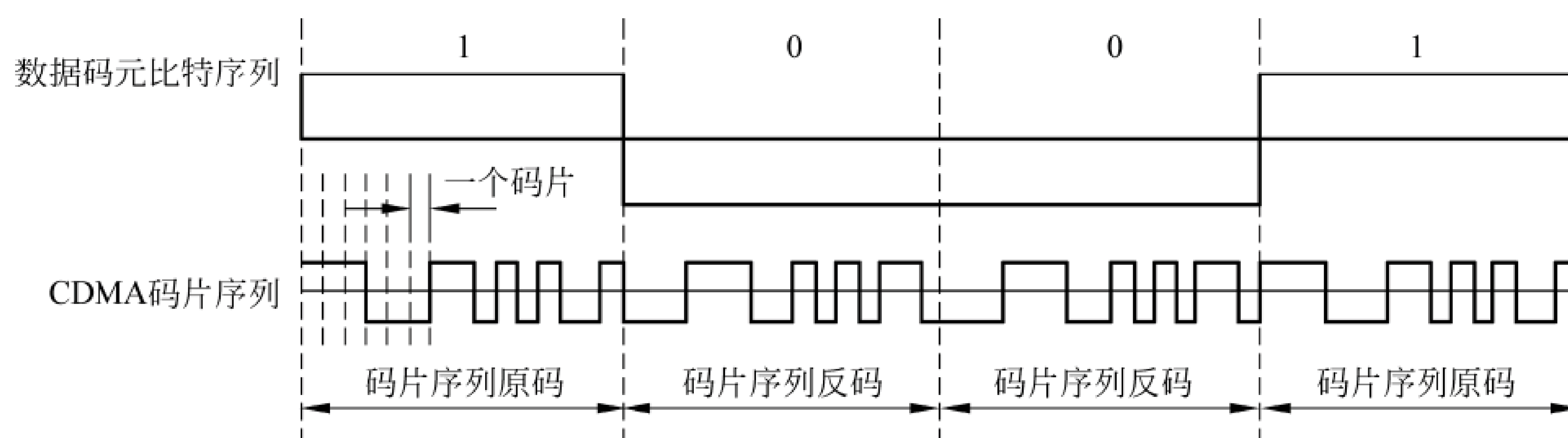


图 1.27　CDMA 的码片序列

实际应用时，码片序列是随机产生的，每一个用户使用不同的码型进行通信，所以具有较高的隐私性能。同时，由于各用户使用的 PN 码都是经过特殊挑选的，因此在同一信道上用同一频率进行传输时，不同码型之间不会相互干扰。

1.3　数据传输控制

1.3.1　数据传输的同步控制

首先引入同步的概念。所谓“同步”，实质上是指为保证数据传输的正确性，收发双方

都以相同的速率来处理（即“发送”与“接收”）数据，从而达到步调一致；否则，数据传输就会出错。比如，如果发送方发送的速率大于接收方接收的速率，则会出现丢包的现象；反之，则会出现重复读取的现象。实现收发双方同步的技术有两种：异步传输和同步传输。

1. 异步传输

异步传输方式又称为起止步传输方式，其特点是传输的数据以字符为单位发送，且字符间的发送时间是异步的，故称为异步传输。其帧结构（见图 1.28）由如下 4 部分组成：

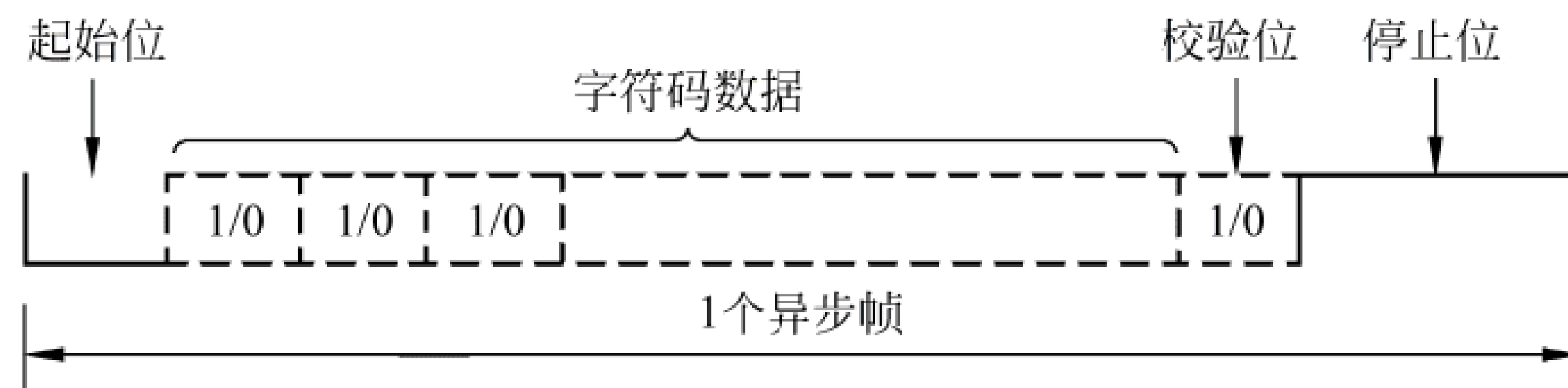


图 1.28　异步传输的帧结构

- 1b 起始位，低电平——数字 0 状态；
- 5b 或 7b 数据；
- 1b 校验位，用作奇偶校验；
- 长度为 1.5b 或 2b 停止位，高电平——也是不通信状态。

在异步传输开始前，传输线上一直处于高电平——不通信状态。当接收端突然检测到传输线上出现低电平时，表明一个字符的起始位到达，接收端利用该位实现与发送端的同步，并顺利地接收其后继的各位。在传输完一个字符之后，停止位到了，线路又恢复到高电平，直到下一个字符到来。异步方式适用于低速设备，其主要优点是实现简单，但效率低，通常用于字节级同步控制。

2. 同步传输

同步传输方式从帧（frame，即数据块）和位两个方面进行传输控制。

1）帧同步的实现

帧同步的实现方法是在数据块的两端加上前文（preamble）和后文（postamble），表示帧的起始和结束。前文和后文的特性取决于所用的协议，并分为面向字符和面向位两大类。

在面向字符的同步传输中，帧头包含一个或多个同步字符——SYN。SYN 是一个控制字符，后面是控制信息和数据字节。接收端发现帧头，便开始接收后面的数据块，直至遇到另一个同步字符。IBM 的二进制同步规程（BSC 或 bisync）是具有代表性的面向字符的同步传输规程。

目前，应用最普遍的面向位的同步传输规程是 ISO 制定的高级数据链路控制协议（High-Level Data Link Control，HDLC）。它把数据块看作数据流，并用序列 0111110 作为开始和结束的标志。为了避免在数据流中出现序列 0111110 时引起混乱，发送方总是在其发送的数据流中每出现 5 个连续的 1 时，就插入一个附加的 0；接收方则每检测到 5 个连续的 1 并且其后有一个 0 时，就删除该 0。如图 1.29 所示为同步传输的两种帧格式。显然，同步

传输的传输效率要比异步传输高。

2）位同步

实现帧同步并不能完全解决传输的同步问题，因为每个帧都比较长，位漂移的积累将使一个帧的后面部分的数据位无法正确接收。为此，还需要实现位的同步。位同步可以通过两种方法进行：外同步法和自同步法。

帧头		控制信息	数据块	校验序列
SYN	SYN	SOH	字符序列	FCS

(a) 面向字符的同步帧格式

帧头	控制信息	数据块	校验序列	帧尾
01111110	C	位流	FCS	01111110

(b) 面向位的同步帧格式

图 1.29　同步传输的两种帧格式

外同步法在发送方和接收方之间提供单独的时钟线路，发送方在每个比特周期都向接收方发送一个同步脉冲。接收端根据这一串同步脉冲来调整自己的接收时序，把接收时钟的重复频率锁定在同步频率上，以便在接收数据的过程中始终与发送端同步。这种方法在短距离传输中比较有效；在长距离传输中，会因同步信号失真而失效。

自同步法利用特殊编码（如曼彻斯特编码或微分曼彻斯特编码）让数据信号携带时钟同步信号，不断校正接收端的定时机构。

同步传输是以位同步为基础，帧同步作为补充的同步控制，其效率较高，但实现比较复杂。

1.3.2　数据传输的差错检测

1. 差错产生的原因与基本对策

在数据通信中，差错的基本应对策略有 3 个。

1）提高信道质量

- 使用高质量的信道：即使用具有热噪声小、信号屏蔽能力强等优点的信道。
- 使用中继器：中继器的作用是每经过一定的传输距离将数据信号重新复制一次。

2）提高数据信号的健壮性

- 纠错码：为传输的数据信号增加冗余码，以便能自动纠正传输差错。
- 检错码：为传输的数据信号增加冗余码，以便查出哪一位出错。

3）采用合适的差错检测技术

与检错码相比，纠错码具有自动纠错功能，但实现复杂、造价高、传输效率低。通常是采用检错码检查出差错，由合适的差错控制协议来补救。

2. 误码检测

误码检测的基本原理是通过在数据部分附加一定数目的冗余码来提供一种检测机制发现传输中的错误。最常用的冗余检错码是奇偶校验、校验和与循环冗余校验码。

1）奇偶校验（odd-even check，Parity checking，parity）

奇偶校验通过向被校验码组中添加 1b（0 或 1），使所有码组的 1 的个数均为奇数或均为偶数，以判断传输中有无错误。通常用于字节为单位的传输中。这时，传输一个字符的 ASCII 码需要 7b，另一位正好用于奇偶校验。

2）校验和（checksum）

为了说明什么是校验和，首先看一个例子：假定要传输的 4 个数字为 1、2、3、5，它们的和为 B（十六进制），则实际发送的是 1235B（将和连同数据一起发送），即

0001 0010 0011 0101 1010

在接收方收到数据后，重新计算一遍数据的和。如果不是 B，则说明传输中发生了错误。使用校验和，计算简单，校验和占用的位数少，但是有时可能出现漏检。如表 1.4 所示，虽然传输中有错误，但接收到的校验和与发送的数据的校验和保持一致。

表 1.4　一个漏检的例子

发送的数据		接收到的数据	
0001	1	0010	2
0010	2	0011	3
0011	3	0101	5
0101	5	0001	1
校验和	B	校验和	B

3）循环冗余码校验（Cyclic Redundancy Check，CRC）

循环冗余码是一种能力相当强的检错码，并且实现编码和检码的电路比较简单，常用于串行传送（二进制位串沿一条信号线逐位传送）的辅助存储器与主机的数据通信和计算机网络中。

循环码通过某种数学运算实现有效信息与校验位之间的循环校验。编码步骤如下：

① 将待编码的 n 位信息码组 $C_{n-1}C_{n-2}\cdots C_i\cdots C_2C_1C_0$ 表达为一个 $n-1$ 阶的多项式 $M(x)$

$$M(x)=C_{n-1}x^{n-1}+C_{n-2}x^{n-2}+\cdots+C_i x^i+\cdots+C_1 x^1+C_0 x^0$$

② 将信息码组左移 k 位，形成 $M(x)\cdot x^k$，即 $n+k$ 位的信息码组

$$C_{n-1+k}C_{n-2+k}\cdots C_{i+k}\cdots C_{2+k}C_{1+k}C_k00\cdots00$$

③ 用 k+1 位的信息码组生成多项式 $G(x)$对 $M(x)\cdot x^k$ 作模 2 除运算，得到一个商 $Q(x)$和一个余数 $R(x)$。显然有：

$$M(x)\cdot x^k=Q(x)\cdot G(x)+R(x)$$

生成多项式 $G(x)$是预先选定的。

模 2 运算是指以按位模 2 加减为基础的四则运算，运算时不考虑进位和借位。模 2 加减的规则为：两数相同为 0，两数相异为 1。模 2 除，就是求用 2 整除所得到的余数，每求一位商应使部分余数减少 1 位。取商的原则是：当部分余数最高位为 1 时，商取 1；当部分余数最高位为 0 时，商取 0。例如

```
                  1 0 1 0 1   -------  商
        ___________________
1 0 0 1 ) 1 0 1 1 1 0 1 0
          1 0 0 1
          -------
            0 1 0 1 ------- 部分余数为010，下1，不足，商中取0
            0 0 0 0
            -------
              1 0 1 0 ------- 部分余数为101，下1，够，商中取1
              1 0 0 1
              -------
                0 1 1 1 ------- 部分余数为011，下1，不足，商中取0
                0 0 0 0
                -------
                  1 1 1 0 ------- 部分余数为111，下0，够，商中取1
                  1 0 0 1
                  -------
                  0 1 1 1 ------- 余数为111
```

④ 将左移 k 位的待编码有效信息与余数 $R(x)$作模 2 加，即形成循环冗余校验码。

例 1.1 对 4 位有效信息 1100 作循环冗余校验码，选择生成多项式 $G(x)$为 1011($k = 3$)。

① $M(x) = x^3+x^2 = 1100$

② $M(x) \cdot x^3 = x^6+x^5 = 1100000$ （k=3，即加了 3 个 0）

③ 模 2 除，$M(x) \cdot x^k/G(x) =1100000/1011 = 1110+010/1011$，即

$$R(x) =010$$

④ 模 2 加，得到循环冗余校验码

$$M(x) \cdot x^3=Q(x) \cdot G(x)+R(x)=1100000+010=1100010$$

下面分析 CRC 的纠错原理。

由于 $M(x) \cdot x^k=Q(x) \cdot G(x)+R(x)$，根据模 2 加的规则：

$$M(x) \cdot x^k+R(x)= Q(x) \cdot G(x)+ R(x)+ R(x)=Q(x) \cdot G(x)$$

合法的循环冗余校验码应当能被生成多项式整除，如果循环冗余校验码不能被生成多项式整除，就说明出现了信息差错。并且有信息差错时，循环冗余校验码被生成多项式整除所得到的余数与出错位有对应关系，因而能确定出错位置。如表 1.5 所示为例 1.1 所得到的循环冗余校验码的出错模式。

表 1.5 循环冗余校验码的出错模式

结果	*D7 D6 D5 D4 D3 D2 D1*	余数	出错位
正确	1 1 0 0 0 1 0	0 0 0	—
错误	1 1 0 0 0 1 1	0 0 1	1
	1 1 0 0 0 0 0	0 1 0	2
	1 1 0 0 1 1 0	1 0 0	3
	1 1 0 1 0 1 0	0 1 1	4
	1 1 1 0 0 1 0	1 1 0	5
	1 0 0 0 0 1 0	1 1 1	6
	0 1 0 0 0 1 0	1 0 1	7

进一步分析还会发现，当循环冗余校验码有 1 位出错时，用生成多项式作模 2 除将得到一个不为 0 的余数，将余数补 0 继续作模 2 除又得到一个不为 0 的余数，再补 0 再作模 2

除……于是余数形成循环。如上例，最终形成 001，010，100，011，110，111，101；001，010，100，011，110，111，101……的余数循环，这也就是“循环码”的来历。

并不是任何一个多项式都可以作为生成多项式。从检错的要求出发，生成多项式应能满足下列要求：

- 任何一位发生错误都应使余数不为 0；
- 不同位发生错误应使余数不同；
- 对余数继续作模 2 运算应使余数循环。

生成多项式的选择主要靠经验。有 3 种多项式已经成为标准，具有极高的检错率，即

$$\text{CRC}-12 = x^{12} + x^{11} + x^3 + x^2 + x + 1$$

$$\text{CRC}-16 = x^{16} + x^{15} + x^2 + 1$$

$$\text{CRC}-\text{ITU}-T = x^{16} + x^{12} + x^5 + 1$$

1.3.3　差错控制

当接收方检测出数据错误后，就不应当接收，而要求发送方重新传输。这种机制称为差错控制。差错控制需要接收与发送双方配合进行，为此需要运行相应的差错控制协议。在差错控制协议中，通常采用自动请求重传（Auto Repeat reQuest，ARQ）机制，即接收方检测出错误后，要求发送方重传出错的数据。

ARQ 的具体实现，可以采用两种不同的策略：停等 ARQ 和连续 ARQ。

1. 停等 ARQ

停等 ARQ（stop-and-wait ARQ）的工作原理如图 1.30 所示。当主机 A 发送一个数据帧到主机 B 时，若 B 正确地收到，便会立即发一个确认应答帧 ACK 给 A，A 接到确认应答帧，就可以再发下一个数据帧；若 B 收到的数据帧不正确，便立即发一个否认应答帧 NAK 给 A，A 接到否认应答帧，就将数据帧重发一次。

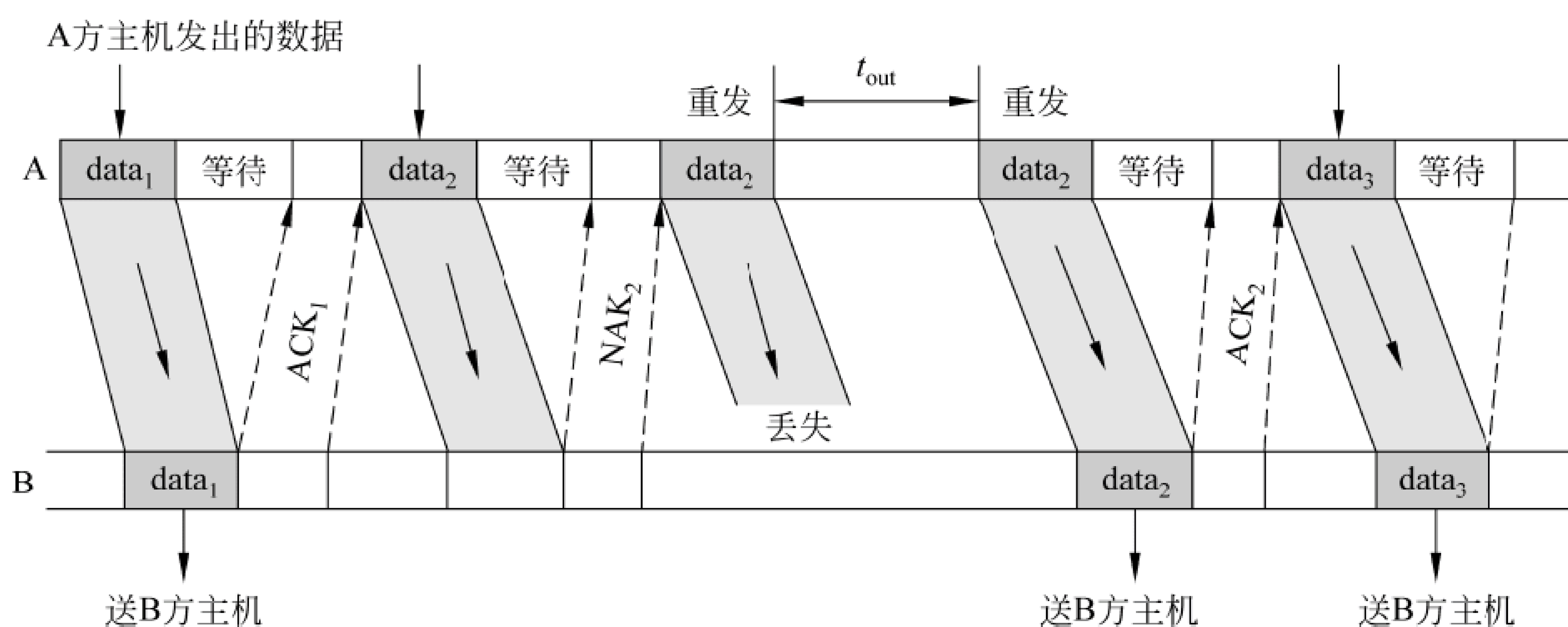


图 1.30　停等 ARQ 的工作原理

此外还有两个问题要解决。

（1）当 A 发出的数据帧丢失，B 收不到时不会发任何应答帧。这时 A 就会一直等待，当等待时间超过一个限度 t_{out} 时，就将数据帧重新发送一次。

（2）B 虽然收到了 A 发来的数据帧，也发出了应答帧（可能是 ACK，也可能是 NAK），

A 却没有收到。在这种情况下，A 等待超过一定时限时，也要将数据帧重新发送一次。

停等 ARQ 协议简单，但系统效率较低。

2. 连续 ARQ

连续 ARQ 是在发完一个数据帧后，不再等待，而是连续地发送若干个数据帧，具体实现方式有拉回（back to N）方式和选择重发（selective repeat）方式。

拉回 ARQ 的工作原理如图 1.31 所示。在发送方 A 连续地发送数据帧的同时，接收方对接收到的数据帧进行校验，并向 A 方发送应答帧；当 A 接收到一个数据帧对应的应答帧为 NAK 时，就从这个数据帧开始将此后所发送过的数据帧重发一遍。例如，A 方发送了 1～5 号数据帧，其中第 2 号数据帧出错，B 将其后已收到的帧（2～5 号）丢弃，A 收到 NAK_2 后，要进行拉回重发。出现超时时，也要拉回重发，如 3 号帧丢失后，要将已发送的 3～6 号帧拉回重发。

图 1.31　连续 ARQ 的工作原理

选择重发 ARQ 与拉回 ARQ 的不同之处在于它只重发出错的数据帧。

3. 重传要求报文分组

差错控制协议的基本原理就是发现错误进行重传。这就要求报文分组。可以想象，如果一个很长的报文，传送用了 10 分钟，结果发现了一个错误，还要用 10 分钟重传，总共要花费 20 分钟。若将报文分成 1000 个分组，还假设发现一个分组有错误，需要进行重传，则总共花费了 10.001 分钟。

1.3.4　数据传输的流量控制与滑动窗口协议

1. 拥塞与死锁

在公路上，车流量超过一定限度，大家的速度就不得不减慢；再超过一定的限度，就会出现谁也走不动的现象。计算机网络也是如此，无论是计算机装置还是通信设备，对数据的处理能力总是有限的。当网上传输的数据量增加到一定程度时，网络的吞吐量下降，这种现象称为“拥塞”（congestion）。传输数据量急剧增加时，丢弃的数据帧不断增加，从而引起更多的重发；重发数据所占用的缓冲区得不到释放，又引起更多的数据帧丢失。这种连

锁反应将很快波及全网，使通信无法进行，网络处于“死锁”（deadlock）状态，陷入瘫痪。

2. 滑动窗口协议

目前，典型的流量控制技术是采用滑动窗口协议。滑动窗口协议是从发送和接收两方的能力来限制用户资源需求，并通过接收方能力来控制发送方的发送数量。其基本思想是：某一时刻，发送方只能发送编号在规定范围内，即落在发送窗口内的几个数据单元，接收方也只能接收编号在规定范围内，即落在接收窗口内的几个数据单元。这不仅可以用于流量控制，还兼有差错控制的功能。

使用滑动窗口协议，要涉及两个方面的问题：

- 数据单元的编号问题（这与数据单元中用于编号的位数有关）；
- 窗口的大小，即缓冲区大小问题。

下面用 3bit（位）进行数据单元的编码，并且发送窗口的大小为 5、接收窗口的大小为 4，来说明滑动窗口协议的工作原理。

1）发送器窗口的工作原理

发送器窗口的大小（宽度）规定了发送方在未接到应答的情况下允许发送的数据单元数。也就是说，窗口中能容纳的逻辑数据单元数就是该窗口的大小。

图 1.32 说明了发送窗口移动的规则，其窗口大小为 5。



(a) 确认单元：0；已发送单元：1，2；未发送单元：3，4，5

(b) 确认单元：1，窗口后沿移动一格；已发送单元：2，3；
未发送单元：4，5；主机传来单元：6；窗口前沿移动一格

(c) 确认单元：3，因单元2未确认，窗口不移动

(d) 确认单元：2，因单元3先前已确认，窗口后沿移动两格；
未发送单元：4，5，6；主机传来单元：7，0，窗口前沿移动两格

(e) 发送单元：4，5，6，且6被先确认

(f) 单元4超时，单元4，5，6重发

图 1.32　发送器窗口的工作原理

2）接收器窗口的工作原理

图 1.33 说明了接收窗口的移动规则，其窗口大小为 4。



图 1.33　接收器窗口的工作原理

前面介绍了用滑动窗口进行流量控制的基本原理，具体实现时还有一些问题要处理，例如：

- 窗口宽度的控制是预先固定，还是可适当调整；
- 窗口位置的移动控制是整体移动，还是顺次移动；
- 接收方的窗口宽度与发送方相同还是不同。

滑动窗口协议不仅可以进行流量控制，也同时可以进行差错控制。

1.4　计算机网络基本工作模式

1.4.1　资源子网的工作方式：客户机/服务器方式与对等方式

如前所述，资源子网主要负责全网的信息处理，为网络用户提供网络服务和资源共享功能等。那么，这个服务的过程是什么样的呢？其实非常简单，要由被服务者向服务方先发出服务请求，服务方在允许的情况下进行响应。按照这样的关系，可以将资源子网中的工作方式为客户-服务器方式和对等方式。

1．对等方式

在对等（Peer to Peer，P2P）方式中，任何一方都可以作主动方，也可以作被动方。或者说，在这种网络中，任何一方都可以先发起请求，所以设备调度配置也基本相当，适合于连接的用户数比较少，且要共享的数据、资源不多的情况。

2．客户-服务器方式

在客户-服务器（Server-Client，C/S）方式中，通信双方的角色被固定为请求方和响应方，分别称为客户方和服务器方。客户方为主动方，只能先发起通信请求；服务器方是被动方，只能响应请求、提供服务。

注意：

（1）这里所说的客户方和服务器方，是对于进程（process）而言的。所谓进程，就是程序的一次运行。所以要使用进程这个概念，是因为现代计算机在操作系统的管理下允许

多个程序并发地工作，包括一个程序多次运行。而每个程序的一次活动，需要一次的活动环境——计算机资源（存储分配等）。为此，在操作系统中把程序关于某数据集合上的一次运行活动称为进程，以其作为资源分配和调度的基本单位。因此，所谓客户方，指的是一个客户进程，服务器方是一个服务进程。不过，在计算机网络中，也把运行服务程序的计算机称为服务器，把只运行客户程序的计算机称为客户端。这样的好处是可以优化资源配置，让运行客户程序的计算机配置低一些，而让运行服务器程序的计算机配置高，使一台服务器可以为多个用户服务，也可以根据服务类型的需要进行计算机的配置。这样，就可以将这两种工作方式用图 1.34 中的两种结构进行表示。

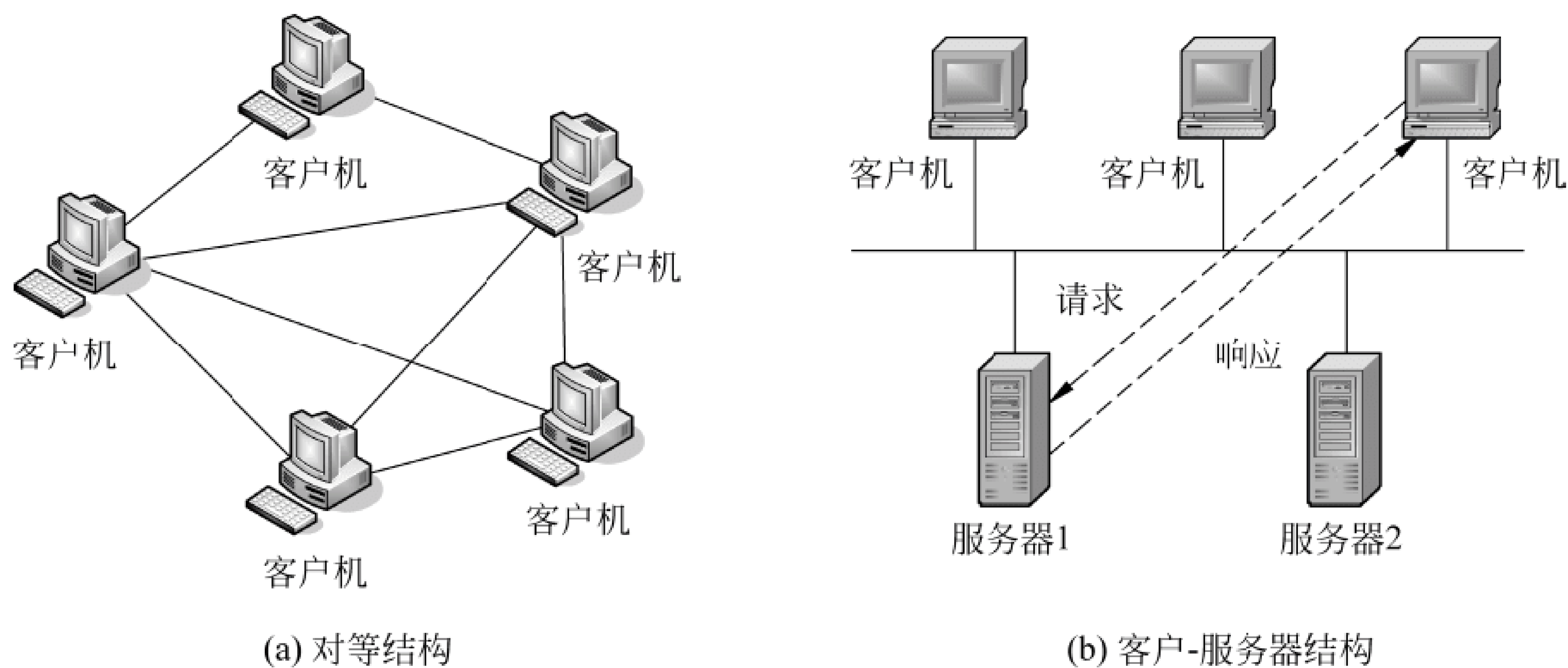


图 1.34　对等结构与客户-服务器结构

（2）在 C/S 模式下，发起通信的主动方是客户，但并非只有一方可以发送另一方只能接收的单工通信；只要通信关系建立，通信就是双向的。哪一方都可以发送，也可以接收。

（3）并非客户端没有计算功能，只有发送请求功能。只是说，服务器端可以提供一些公共服务，如数据库检索等。

（4）如图 1.34 所示的两种结构，不是物理结构，而是逻辑结构，只是用来表示计算机之间的工作关系，也称为两种工作模式。

3．C/S 计算模式的优点

目前的计算机网络基本上都是采用 C/S 模式的，原因就是它能带来如下一些益处。

（1）增强了系统的稳定性和灵活性。C/S 模式将应用与服务相分离，使得系统具有即插即用的特点，减少了因系统变更带来的影响，模块易于替换、增减、移植，增强了系统的稳定性和灵活性。

（2）能够为作业配备较佳资源。C/S 模式可以针对应用和服务的不同要求，以及针对不同的处理要求来配置相应的资源，取得最佳的性能/价格比，提高了服务质量、集成水平和事务处理能力。

（3）大大减低了系统的开发成本和风险。C/S 模式便于类似系统的开发，它提供了一个开发框架，缩短了解决问题的时间，减少了风险，有利于快速解决问题，能将开发过程中的重复劳动减小到最少。同时，它可以在较低廉的工作站上完成开发，然后移植到较昂贵

的产品系统中，大大减少了开发费用。

（4）便于维护和应用。C/S 模式为系统人员提供了一个共同的后台（服务器）环境，为用户提供了一个友好的操作环境，便于维护和使用。

如上述所述，由于 C/S 模式可以进行系统的合理配置，也便于维护，特别适合计算机网络中各种应用，如域名服务、E-mail 服务、Web 服务等。到了 20 世纪 90 年代中期，客户端逐渐变成了只运行浏览器，并把这种模式称为 B/S（Browser-Sever，浏览器-服务器）模式。

1.4.2　数据传输的关键技术：分组交换

1. 广播与交换

由通信子网的拓扑结构可以看到，一个结点往往连接着几条链路。这样，可以抽象为两种基本传播形式：广播（broadcast）与交换（switching）。

广播是从一条链路传来的信号，将被复制到其他链路。交换是将从一条链路传来的信号有选择地传送到其他一条或几条链路上。总线和环形拓扑一定是广播方式，而星形和树形拓扑则因结点上的通信控制处理器而异：若结点上的通信控制处理设备是中继设备，则其传播是广播方式；若结点上的通信控制处理设备是交换设备，则其传播是交换方式。

交换的基本功能就是转发业务流。交换是通过交换结点中的交换机构实现的。如图 1.35 所示，交换机构的功能是将一条输入信道上的数据转送到另外的输出信道上，将输入端口与输出端口对应起来。

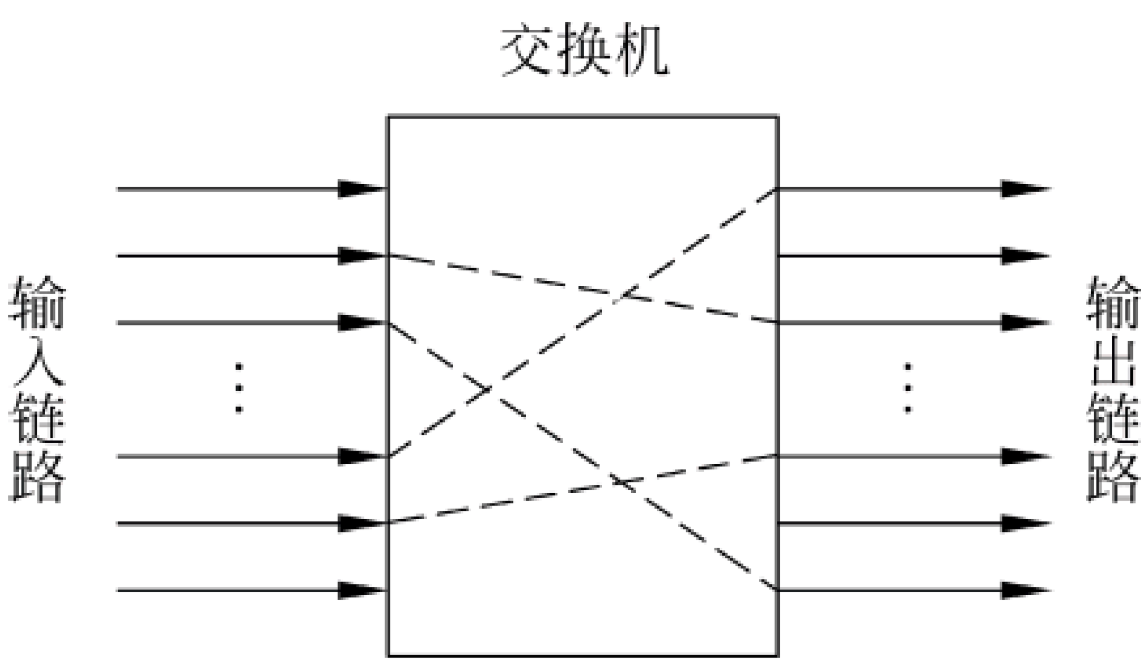


图 1.35　交换设备的功能

在多结点网络中，一个通信过程往往要经过多条链路之间的转接才能实现。在图 1.36 中，结点 A 到结点 B 之间的通信，要经过一系列中间结点的转接。转接由交换结点实现。

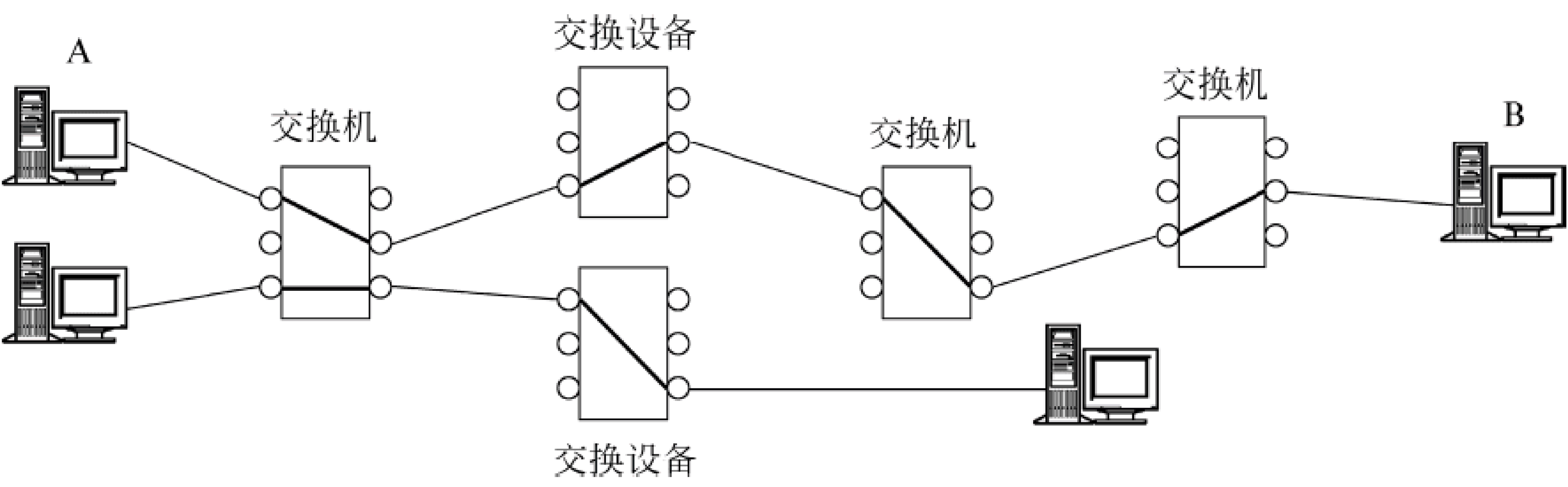


图 1.36　通过交换结点连接的通信

2. 从电路交换到分组交换

1）电路交换

电路交换（circuit switching 或 circuit exchanging）就是使用交换开关进行物理信道的交

换，将通信双方的多条链路连接成一条专用的通道，是早期的数据交换方式。采用电路交换方式，通信的双方在进行数据传送之前先要建立一个实际的物理电路连接，连接的电路被通信的一对用户独占，并且这种连接要持续到双方通信结束，只有通信结束电路释放后，才能被别人使用。简单地说，它要经过 3 步：建立连接（呼叫）、数据传送、线路拆除（释放）。在通信过程中，交换机为通信双方提供物理电路连接，如图 1.37 所示，如果 H_1 要与 H_5 经过交换结点 A、B 和 E 通信，则 AB、BE 这两段链路在 H_2 与 H_5 通信期间是不能被别人使用的。

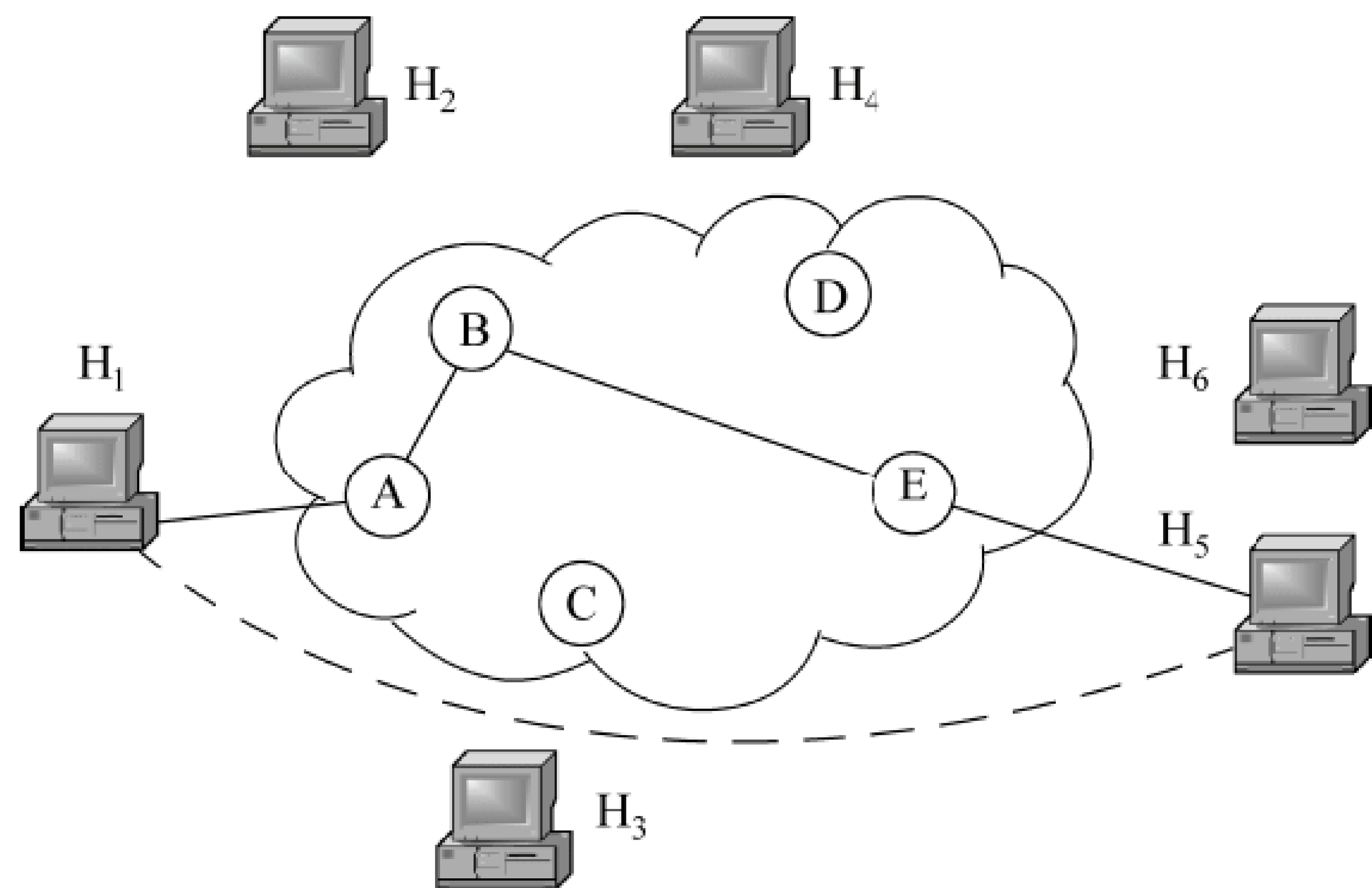


图 1.37　电路交换示意图

电路交换具有如下优点：

（1）由于通信线路为通信双方用户专用，数据直达，所以传输数据的时延非常小。图 1.38 为电路交换在数据传输时的时间关系。

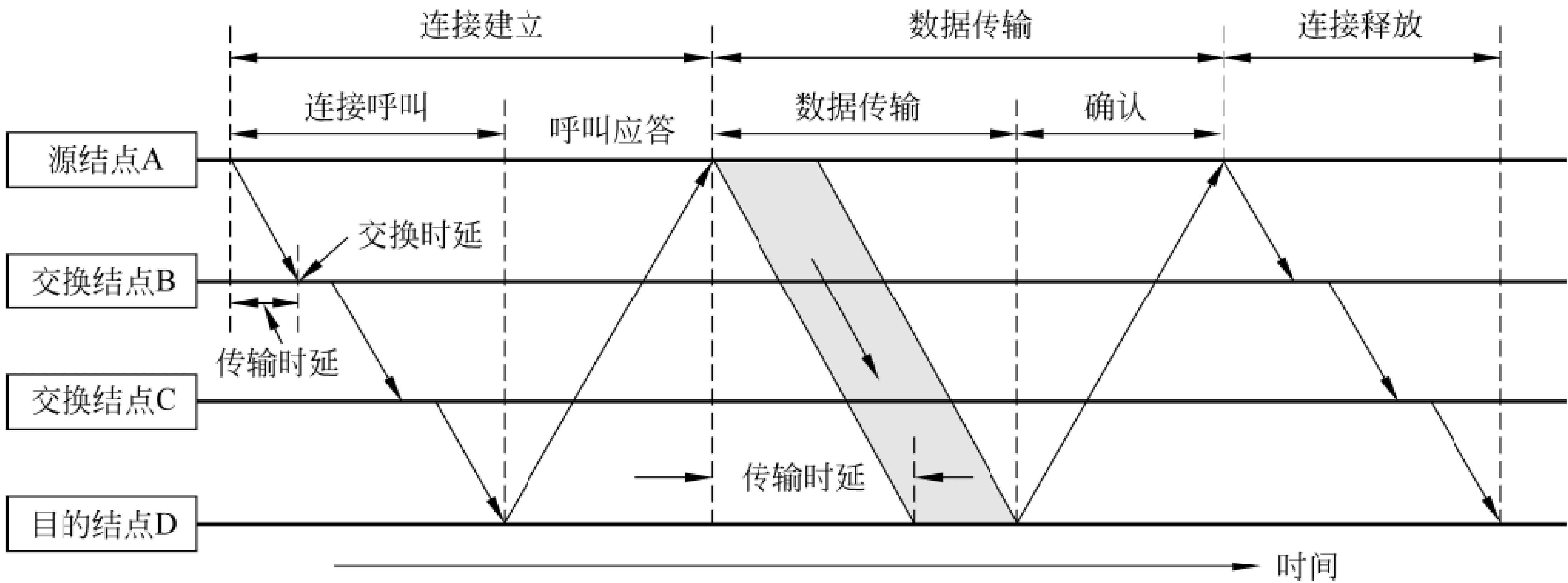


图 1.38　电路交换的基本过程

（2）通信双方之间的物理通路一旦建立，双方可以随时通信，实时性强。

（3）双方通信时按发送顺序传送数据，不存在失序问题。

电路交换具有如下缺点：

（1）电路交换连接建立后，物理通路被通信双方独占，即使通信线路空闲，也不能供其他用户使用，因而信道利用率低，也会因此造成数据传输中的拥塞。

（2）由于需要连接过程，而建立连接需要时间，故适合传输大量数据，在传输少量数据时效率不高，不太适合数据量不确定的计算机通信。

（3）电路交换时，数据直达，不同类型、不同规格、不同速率的终端很难相互进行通

信，也难以在通信过程中进行差错控制。

2）*存储-转发交换*

随着数字技术的成熟，存储-转发交换（Store-and-Forward Switching）被应用到了数据交换中。存储-转发是一种不要求建立专用物理信道的交换技术。当发送方要发送信息时，应把目的地址先加到报文中，然后从发送结点起，按地址把报文一个结点、一个结点地转送到目的结点；在转送过程中，中间结点要先把报文暂时存储起来，然后在线路不忙时将报文转发出去，这就是将其称为存储-转发交换的缘由。存储转发交换不像电路交换那样要独占一条固定的信道，线路利用率高，同时可以根据网络中的流量分布动态地选择报文的通过路径，系统效率高，因而得到了广泛的应用。如图 1.39 所示，由于在存储-转发交换中，H_1—H_5 间的数据通信与 H_2—H_6 间的数据通信，可以共用 B—E 段链路，只要它们不同时在这段链路上传送，就没有关系。即使两个报文同时到达结点 B，也可以先存储在缓冲区内，排队发送。

早期的存储-转发交换以报文（message）形式进行，称为报文交换。图 1.40 演示了在连续的 4 个结点之间用报文交换方式进行数据传输的基本过程。可以看出，接收端每收到一个报文，都要进行校验并确认。为了实现存储-转发，每个交换结点要为每一个端口分别设置一个输入缓冲区和一个输出缓冲区。

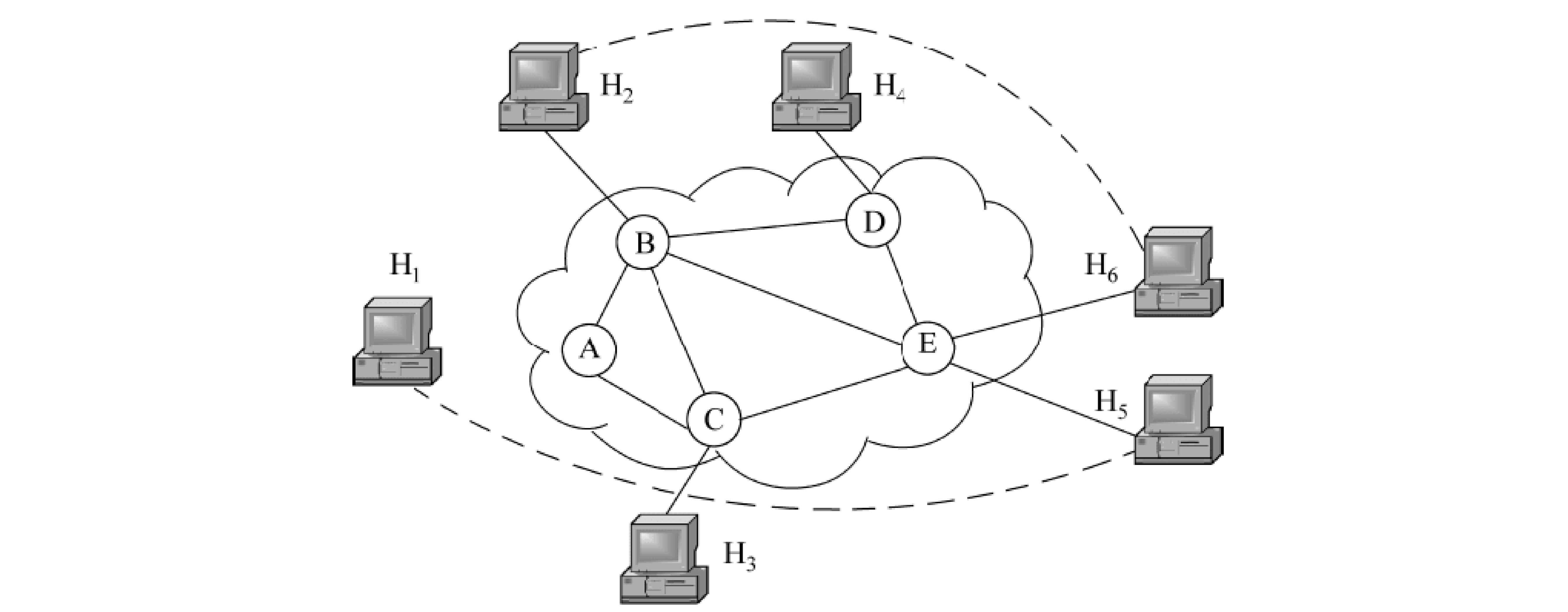


图 1.39　存储-转发交换示意图

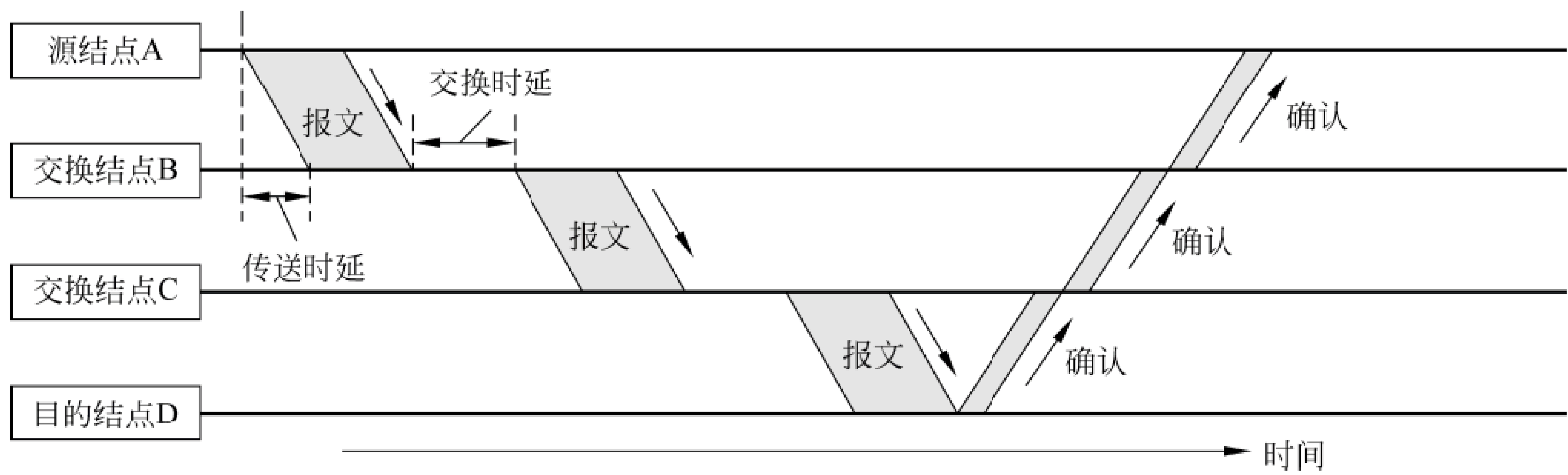


图 1.40　报文交换的基本过程

这里，处理时延是结点为存储转发处理所花费的时间；发送延时是结点使报文的第一字节进入传输媒体到全部报文进入传输媒体所需要的时间。显然，当报文较大时，处理时

延和发送延时会较长。同时报文较长，在传输过程中会由于个别字节错误而导致整个报文传输作废。例如，某一线路允许的差错率为 10^{-5}，若传输的报文长度为 100KB，则每次传输中都可能有 1 个字节出错。这样的报文很难传到目的结点。为此，在报文交换的基础上，多纳德·戴维斯（Donald Davies）和保罗·巴兰（Paul Baran）在 20 世纪 60 年代早期研制出分组交换（packet switching）技术。

3）分组交换

分组交换也称包交换，就是按一定长度将报文分割为许多小段的数据——分组，每个分组独立进行传送。在分组交换网中，要先把一个报文分割成规定长度的信息组——分组打包，然后在每个分组上贴上标签——报头，按编号一批一批地将“数据分组”发出去；在每一个中间结点上，都要先存储、后转发；传送到达目的地后，再重新装配成完整的报文。图 1.41 为报文分组的示意图。

在不同的分组交换网络中，会定义不同的帧长度，也会有不同的传输效率。图 1.42 为分组在一个具有 A、B、E 三个中间结点的网络中连续传输分组时的情形。假设每个网段的传输时延相同，则当分组缩短到 1/4 时（见图 1.42（b）），传输两个网段，比原来（见图 1.42（a））缩短了 3/4 个帧发送时间 τ_{A1}，即每多传一个网段只会增添 1/4。

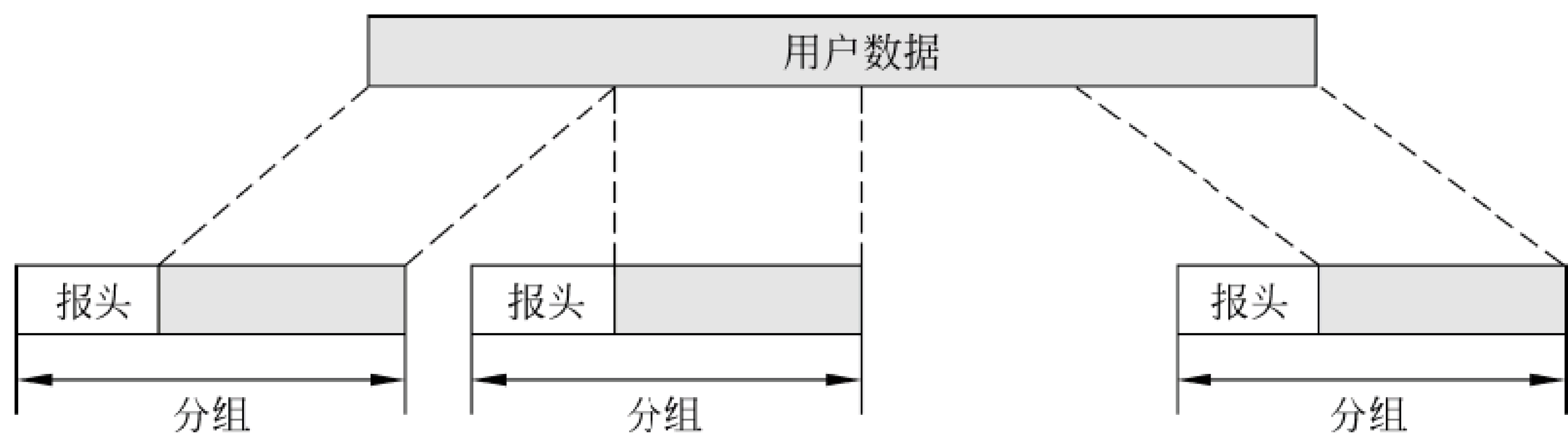
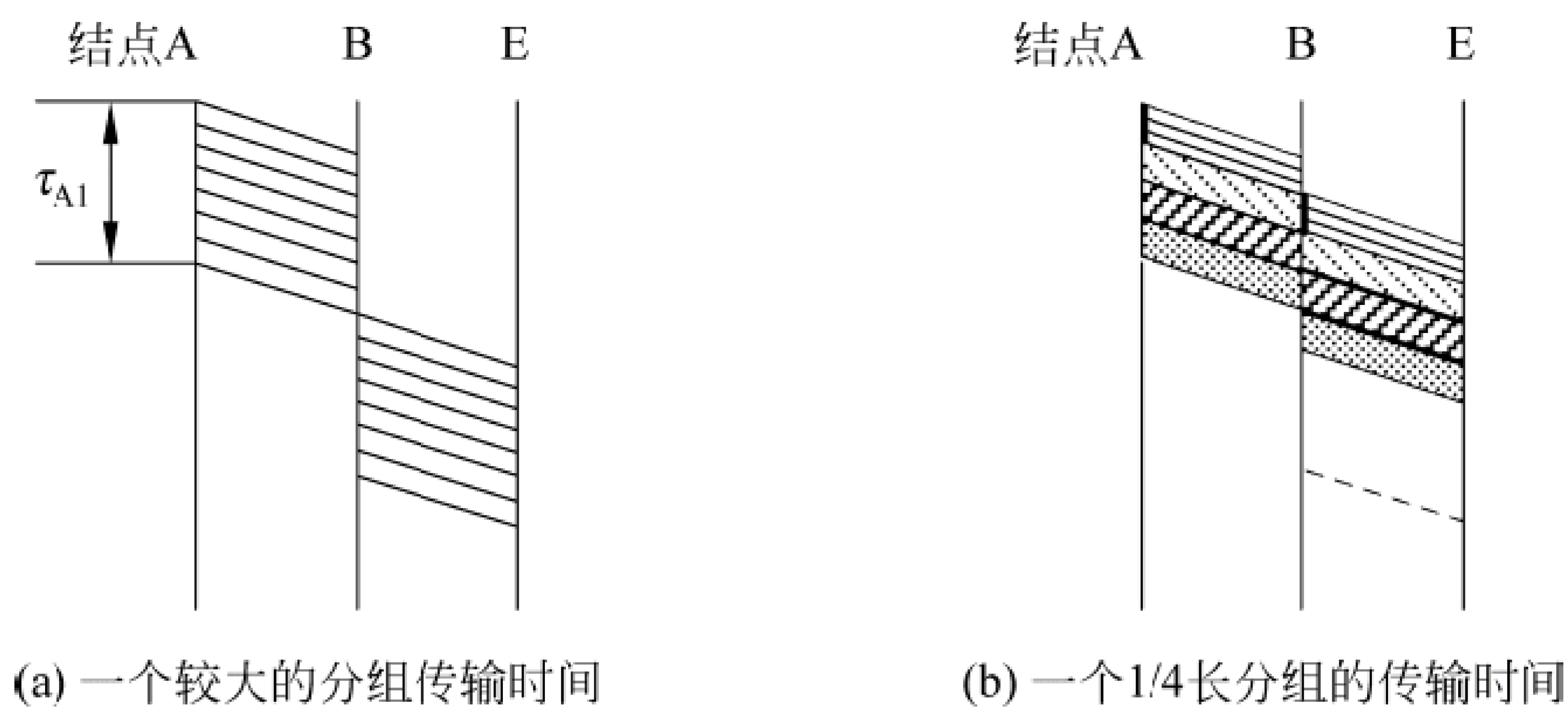


图 1.41　报文分组



(a) 一个较大的分组传输时间　　(b) 一个1/4长分组的传输时间

图 1.42　不同长度分组对传输过程的影响

与报文交换相比，分组交换的优点是：

（1）在报文交换中，总的传输时延是每个结点上接收与转发整个报文时延的总和；而在分组交换中，某个分组发送给一个结点后，就可以接着发送下一个分组，形成多个分组时延重迭，这样总的时延就会减小；

（2）每个中间结点只需存储分组，使所需要的缓存器容量减小，这有利于提高结点存储资源的利用率；

（3）传输有差错时，只要重发一个或若干个分组，不必重发整个报文，提高了传输

效率。

分组交换的缺点是每个分组都要从运输层向下层进行打包，增加头、尾。所以分组长度过小，不仅会使网络传输开销过多地花费在控制信息方面，还会增加各结点的负荷处理量。因此，最佳帧长度的选择是传输时间、传输开销和网络处理负荷之间的折中。

1.4.3　分组传输模式：虚电路与数据报

报文分组之后，在网络中可以用两种不同的模式传输：虚电路（virtual circuit）和数据报（datagram）。

1. 虚电路

虚电路类似于一个部队要转移时，先派出侦察兵侦察好一条通道，然后部队有序地沿着这条通道转移。在虚电路上进行数据传送，就是所有的数据段都要从这条信道上有序地传输。之所以加了“虚”字，是因为两个原因：一是这条信道不是永久的，在传送前要先建立连接，传送后就释放这个连接；二是不固定，如在图 1.38 中，H_1 要与 H_5 通信，这次是走 A—B—E，下次可能是 A—C—E，再下次可能是 A—B—C—E。当然，也可以用后不拆除，后面继续使用。这种不拆除的虚电路称为永久性虚电路(PVC)。而用后就拆除的虚电路称为交换虚电路（SVC）。

虚电路传输的特点是：

（1）有一个连接—通信—拆除的过程（如图 1.43 所示）。

（2）报文段的顺序保持，不被打乱。

（3）传输较长报文时，效率较高。

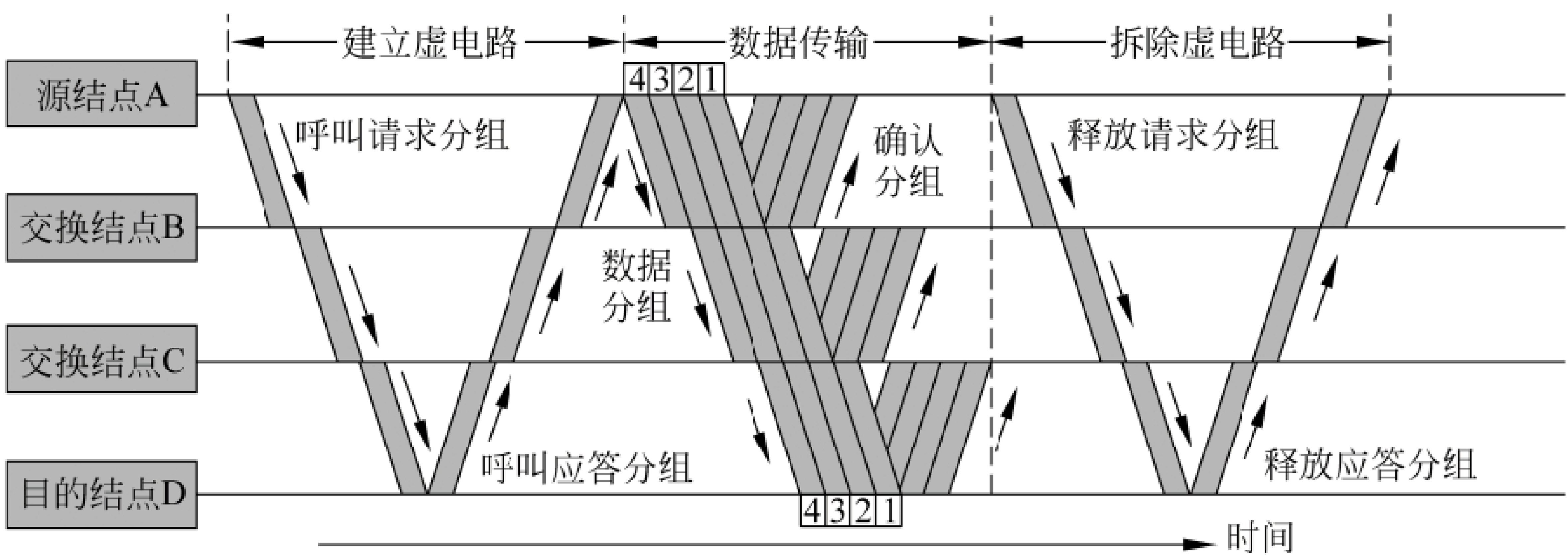


图 1.43　虚电路中的分组传输

2. 数据报

如图 1.44 所示，数据报类似于一个大部队要转移时，先原地解散，然后各自寻找路径，到规定地点集合。按照这样的模式，每个数据分组均带有发信端和收信端的全网络地址，一个分组到达某个结点时，该结点交换机都会按照当时的情况为其选择一条合适的路径。这样就形成不同分组沿不同路径传播的情形，并且到达目的端点后的接收顺序与发送顺序会有不同，收信端必须对接收的分组进行顺序化，才能恢复成原来的电文。数据报方式比较适合于传输只包含单个分组的短电文，如状态信息、控制信息等。

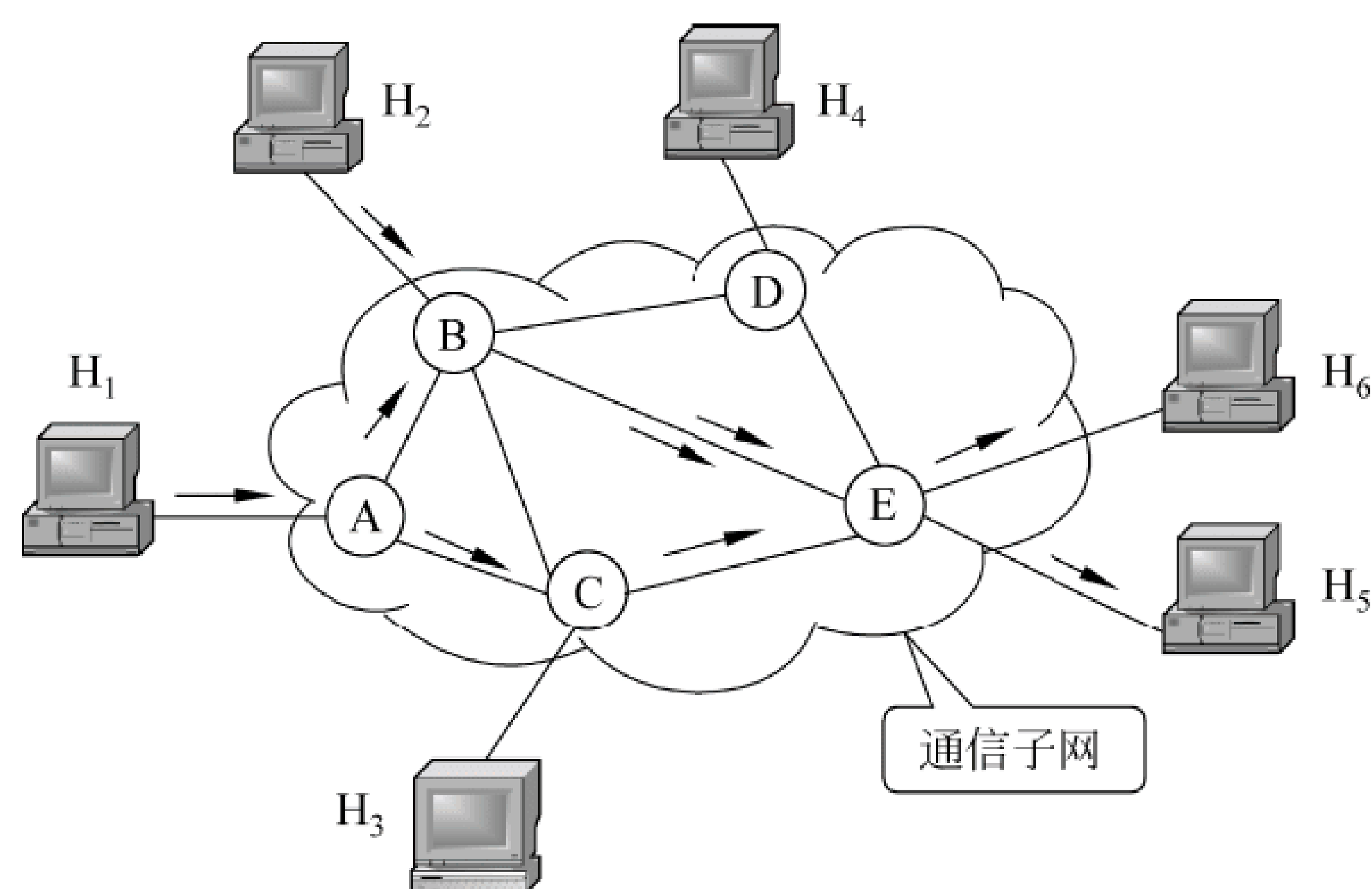


图 1.44　数据报传输方式

表 1.6 为两种服务方式的比较。

表 1.6　虚电路服务和数据报服务的对比

对比内容	虚电路服务	数据报服务
基本思路	可靠通信应当由网络来保证	可靠通信应当由用户主机来保证
连接的建立	必须有	不需要
终点地址	仅用于连接建立阶段，各分组使用短的虚电路号	每个分组都有终点的完整地址
分组的转发	属同一条虚电路的分组均按照同一路由进行转发	每个分组独立选择路由进行转发
当结点出故障时	所有通过故障结点的虚电路均不能工作	出故障的结点可能会丢失分组，一些路由可能发生变化
分组的顺序	总是按发送顺序到达终点	不一定按发送顺序到达终点
端到端差错处理和流量控制	可以由网络负责，也可以由用户主机负责	由用户主机负责

1.5　计算机网络法定标准——ISO/OSI-RM 模型

20 世纪 50 年代初，美国为了自身的安全，在美国本土北部和加拿大境内建立了一个半自动地面防空系统 SAGE（赛其系统），在这个项目中进行了计算机技术与通信技术相结合的尝试。从此，开创了一条通向计算机网络的先河。20 世纪 70 年代末期，计算机网络已经势不可当。面对这样的潮流，为了抢占这一制高点，IBM 公司于 1974 年公布了 SNA（IBM Systems Network Architecture，IBM 系统网络体系结构）模型，其他商家也相继推出了自己的网络体系，如 DEC 的数字网络体系结构 DNA（Digital Network Architecture）、UNIVAC 的分布式计算机体系结构 DCA、美国国防部的 TCP/IP 等。这些计算机网络基于不同的设计思路和技术，采用了不同的网络体系结构，各有自己的协议体系。这种山头林立的局面给网络互联和进一步发展造成了很大障碍。

为了促进计算机网络的发展，国际标准化组织（International Organization for Standardization，ISO）于 1977 年成立了一个委员会，着手在已有网络的基础上，建立一个不基于具体机型、操作系统或公司的网络体系结构。1982 年 4 月形成并发布了一个开放系统互连参考模型（Open System Interconnection-Reference Model，OSI-RM）的国际标准草案。

1.5.1 基于层次结构的实体、协议、服务和访问点

1．分层结构

模块化和分层是分析、设计和构造复杂系统的有效手段。计算机网络是一种复杂系统，因此 OSI-RM 也采用了分层结构。如图 1.45 所示，OSI-RM 分为物理层（Physical Layer，PHL）、数据链路层（Data Link Layer，DL）、网络层（Network Layer，NL）、运输层（Transport Layer，TL）、会话层（Session Layer，SL）、表示层（Presentation Layer，PL）和应用层（Application Layer，AL）。

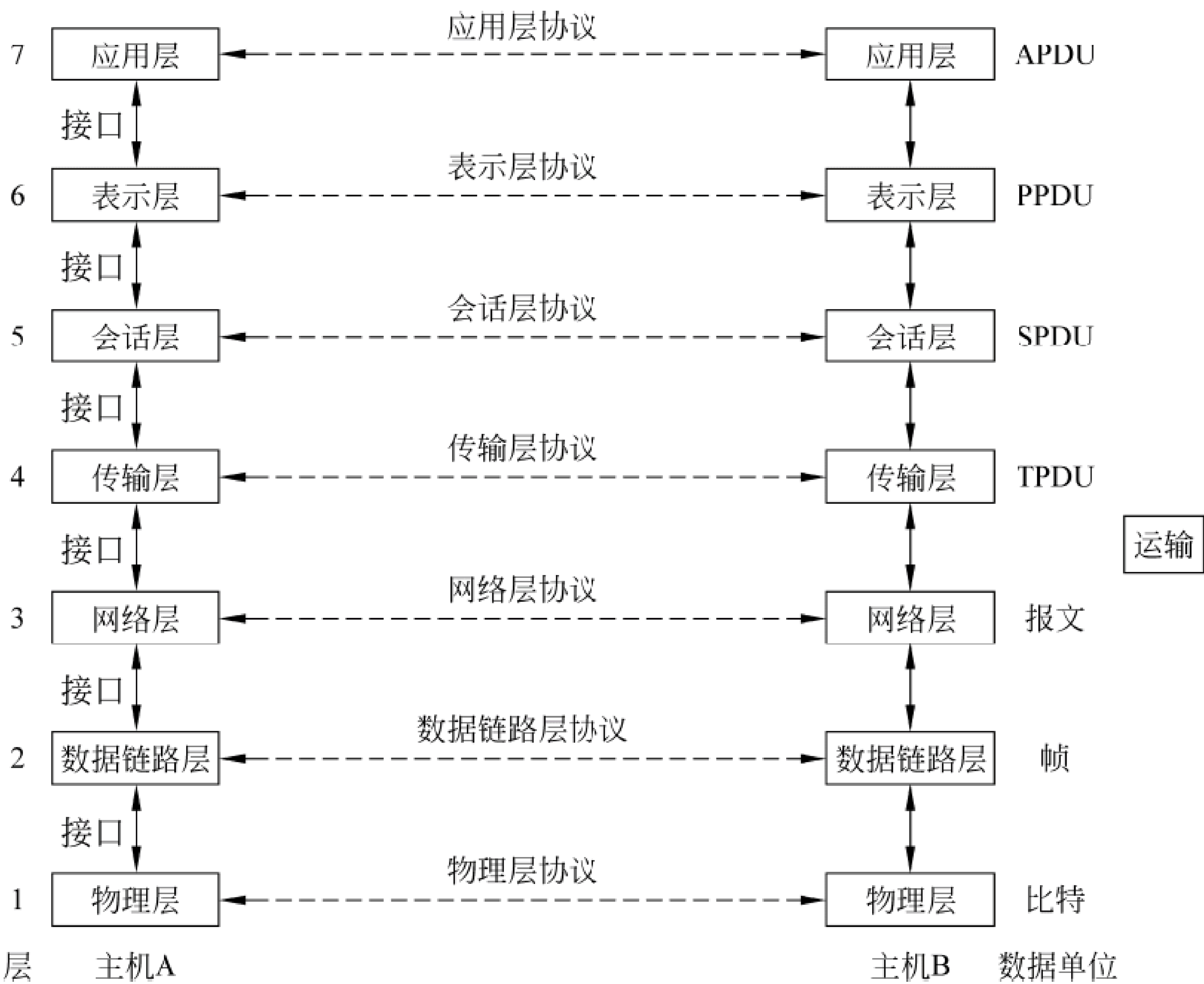


图 1.45　OSI/RM 模型

2．4 个核心概念

OSI/RM 仅仅是一个参考模型，并非一个真实的计算机网络体系，可是多年来，它一直被人们作为理解计算机网络原理、设计新产品的指导理论，不仅因为它采用了分层结构，更重要的是它定义了网络中的 4 个核心概念：实体、协议、服务和访问点。

1）实体

OSI/RM 把每一层中担任发送或接收信息的硬件或软件进程的抽象，如集线器、网卡、交换机、路由器以及有关软件进程都抽象为实体（entity）。实体是网络的基础，网络的所有活动都是实体活动的表现。

作为一种抽象概念，在不同角度，在抽象层次上，实体的含义有所不同。例如，从作用上，在计算机网络中活动的实体主要是两类：用户实体和资源实体。用户实体（如用户程序和终端等）以直接或间接方式与用户相联系，反映用户所要完成的任务和服务请求。资源实体（如设备、文档和软件系统等）与特定的资源相联系，为用户实体访问相应的资

源提供服务。

在计算机网络中，实体之间有两种关系：对等层之间的关系和相邻层之间的关系。

2）协议

网络协议（network protocol）简称协议，是网络中对等实体之间关系的限定、控制或定义。因此，每一层都有相应的协议进行通信的控制。如图 1.45 所示，在 OSI/RM 中，存在 7 大类协议：物理层协议、数据链路层协议、网络层协议、运输层协议、会话层协议、表示层协议和应用层协议。当然，每一层都有一些子协议。

协议就是保证通信系统可以正常、有效工作的一些协调机制，它们要求有关元素必须遵守约定的规程和规则。简单地说，协议是进行通信的规则、约定或规则。网络中的实体活动必须共同遵守的一些规则和约定，才能相互合作，完成共同关心的任务。

协议存在于任何通信过程中，它包含了语义、语法和规程三个方面的约束。

（1）语义：即相互通信的内容含义。简单地可以说是“表达什么”。

（2）语法：关于信息格式的规定。简单地说是关于“如何表达”的规则。因为在计算机网络中传输的信号是一些二进制比特流，为了让系统能够识别这些比特流，需要将信息按一定的格式进行组织和传输。例如，一个数据分组有多长，具体划分为几个字段等。两个不同的网络互联，即当一个数据分组被转换为数字信号以后从一个网络进入另一个网络时，必须进行数据格式的转换，这就需要根据两种网络协议的规定进行数据的分割与组装。

（3）规程：用于规定交互的时间和顺序关系。例如，接到请求，就是响应。与打电话一样，听到了呼叫铃声，再去接听。如果没有铃声就接听，不仅听不到对方请求，还屏蔽了一切来电。

3）服务

服务（service）用于定义层次结构中一方实体对于其上层实体的支持关系。在计算机网络中，每一层的工作都是在协议的控制下，在下一层提供的服务基础上进行的。或者说，某一层要实现本层协议，还需要使用下面一层所提供的服务，并且下层的协议实现对这一层是透明的，即这一层不需要知道协议层协议的实现细节。例如，物理层是在传输介质提供的服务上进行的，数据链路层是在物理层提供的服务的基础上进行的，但不需要知道物理层协议是如何实现的。

所以，协议是实体之间的水平关系，服务是实体之间的垂直关系。

4）服务访问点

服务访问点（Service Access Point，SAP）是指层间接口，是同一系统中相邻两层的实体间交互（即交换信息）的地方。

1.5.2 OSI/RM 标准的制定原则

1. OSI/RM 的三级抽象

在 OSI 标准的制定过程中，所采用的方法是将整个庞大而复杂的问题逐步细化，并从三个抽象层次上进行考虑。

第一个层次的抽象是定义体系结构。计算机网络体系结构是对计算机网络的各层功能

精确定义及其各层遵守协议的集合。OSI 体系结构也就是 OSI 参考模型，它描述了各层的功能以及各对等层之间的协议关系，形成一个关于计算机网络的基本概念。

第二层次的抽象是定义服务。服务定义就是较详细地定义各层所提供的服务。这些功能将通过接口提供给其上层，来保证上层的功能，各层所提供的服务与这些服务是怎样实现的无关。此外，各种服务还定义了层与层之间的抽象接口，以及各层为进行层与层之间的交互而用的服务原语（指下层协议通过接口为上层协议提供某种服务而发送的一组指令是不同层间的通信语言）。但这并不涉及这个接口是怎样实现的。

第三层次的抽象是定义 OSI 协议规范，各层的协议规范精确的定义是：应当发送什么样的控制信息，以及应当用什么样的过程来解释这个控制信息。协议的规范是对计算机网络各个部分严格的约束。

2．OSI/RM 的层次划分原则

（1）网路中各结点都有相同的层次；

（2）不同结点的同等层具有相同的功能；

（3）不同结点的同等层按照协议实现对等层之间的通信；

（4）同一结点内相邻层之间通过接口通信；

（5）每一层使用下层提供的服务，并向其上层提供透明服务。

在 OSI/RM 模型中，低三层可以划做通信子网，高三层可以划做资源子网，运输层则是一个承上启下的层次，有人将其划做资源子网，也有人将其划做通信子网，其实都没有关系，通过下一阶段学习，读者可以自己判断一下它到底划到哪个子网合适。

3．数据打包与拆包

在发送端，数据从顶层开始，层层打包，最后送到物理介质中传输；数据从发送端的物理层传输到接收端的物理层后，向上层层拆包交给接收端的应用层处理。

1.5.3　OSI/RM 体系工作机理

OSI/RM 的工作机理可以用图 1.46 粗略描述。为了便于理解 OSI/RM 各层的功能，下面自顶向下地介绍。由于顶层为第 7 层，所以下面用段号表示层号。

7．应用层

应用层是 OSI/RM 中的最高层，是用户与网络的接口。它用于接收应用程序的数据报文（message），如要传输的一个文件、一封电子邮件等。由于应用进程分为客户端与服务器端两种类型，应用层会提供对这两种进程之间的支持和服务，并分别生成请求报文与应答报文进行交互。它们都是应用层的数据报文。

这些报文经过网络传送到接收方后，接收方的应用层要知道这些报文是做什么的等信息，不然对接收方毫无用处。为此，发送方要在应用程序生成的报文上，再附加一些信息，形成应用层数据报文。这些附加信息称为应用层报文首部，相当于寄信时的信封。在图 1.46 中用 H7（也可以写作 AH）表示。

6. 表示层

应用层产生数据报文后，先到表示层要解决在网络中进行传输时采用什么样的编码形式的问题。具体包括了如下内容：

（1）采用哪种编码，是 ASCII 码，还是 Unicode 等。

（2）数据之间有什么关系——数据结构问题。

（3）要不要加密传输：若要加密，采用什么样的加密算法和密钥。

（4）要不要压缩传输：若要压缩，采用什么样的算法。

这 4 个方面合起来就称为数据报文的表示问题。发送方是这样表示的，到了接收端，还必须知道发送方是如何表示的。因此，发送方的表示层除了要对应用层传下来的应用层报文进行表示变换外，还要附加上一些信息，说明这些表示的方法，并打包成一个新的表示层数据报文。这些在表示分层附加的信息称为表示层报文头，在图 1.46 中用 H_6（也可以写作 PH）表示。

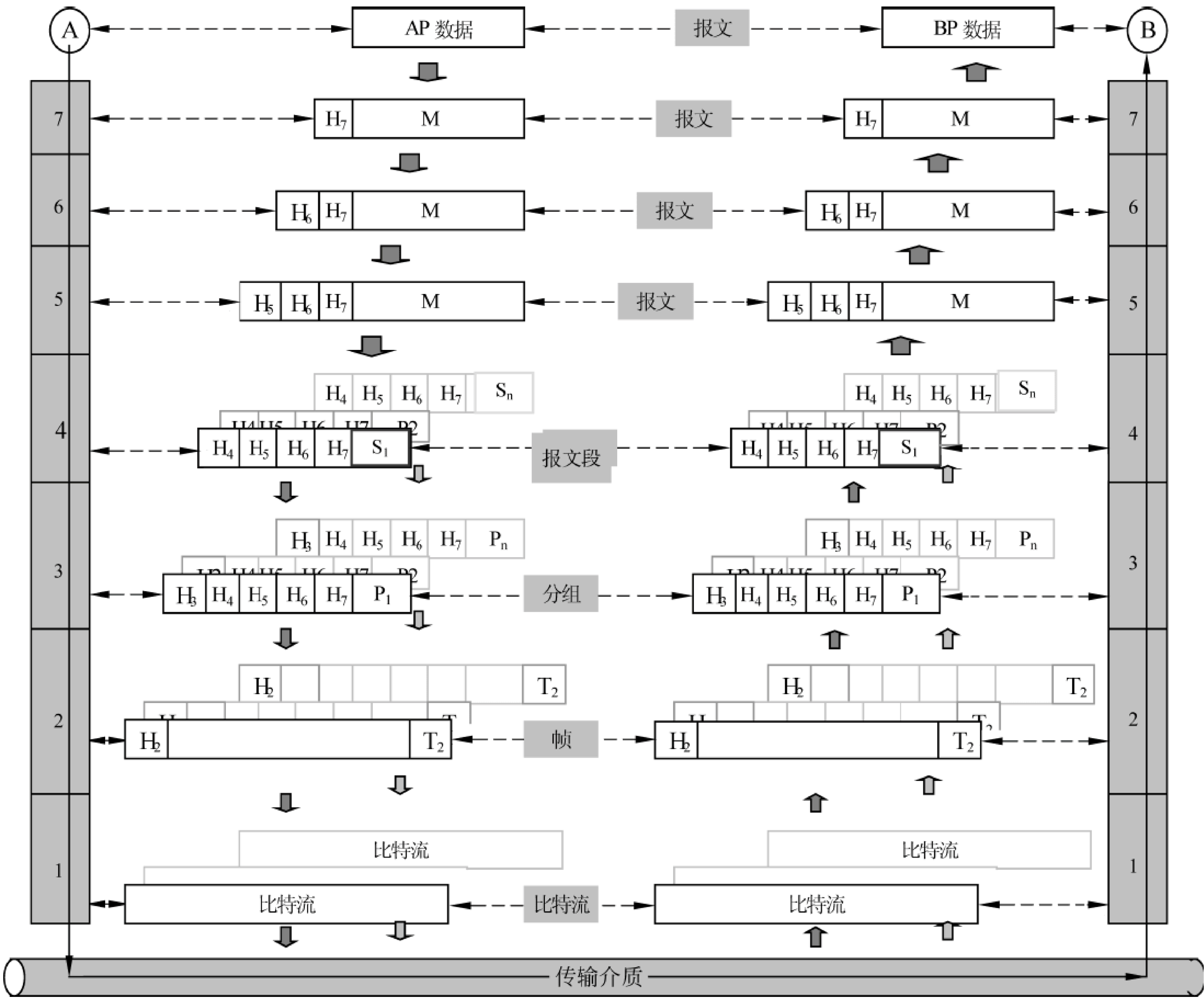


图 1.46　OSI/RM 工作机理

5. 会话层

在表示层形成表示层数据报文后，并不能直接放到网上，还必须在发收双方进程建立

了会话以后才可以发送。为此要有一个会话层，进行会话管理，包括：

（1）双方会话是同时双向，还是只许轮流单向。

（2）当有多对用户进行通信，而共用一条链路时，如何会话而不串音。

（3）一个大的数据报文的传输中发生断线，是重传，还是接着传。

与应用层和表示层一样，为了说明会话采取的方法，发送方的会话层也要再加上一个报头，在图 1.46 中用 H5（也可以写作 SH）表示。

4．运输层

运输层是计算机网络中的关键一层，其上属于资源子网，用于生成数据报文；其下属于通信子网，用于进行数据传输。在资源子网中活动的实体是进程：数据报文是由位于源主机上的某种应用进程（程序运行）发出，由位于目的主机上的相关进程接收的。运输层的基本职责是把应用进程生成的报文交到通信子网传输。为此，它把源进程和目的进程之间的通信子网看作一条链路，具体这个通信子网如何工作，那不是它的事，要由下层一步一步地实现。也就是说，它把通信子网看成一条信道，并且是在下层服务的支持下工作的。这样，进程间的通信就变成了一条链路两端的两个结点之间的通信。而这种通信，要涉及如下问题：

（1）上层交来的数据报文是由哪种应用程序的进程产生的。

（2）数据传输时的差错控制问题。

（3）发送端的发送能力和接收端的接收能力——报文分片（段）、流量控制和拥塞控制。

（4）由于上层有多个应用进程，所传输的报文属于多个进程，要在一条链路中传输，涉及多路复用。

（5）多路复用、差错控制以及网络中的交换，都要求不能以整个报文进行传输，所以需要把上层交来的报文进行分段。在源段分段之后，到了目的端，还有整序组装的问题。

（6）这个信道是虚电路方式，还是数据报方式。

所有关于上述问题的约定，就是运输层协议的内容。为此，在运输层要在上层交来的数据报文之上，再添加有关上述约定的信息，这就是图 1.46 中的 H4（也可以写作 TH）。

3．网络层

运输层要解决的进程间通信是在网络层提供的服务的基础上进行的。由于应用进程运行在网络主机上，所以，网络层是处理主机之间的通信问题。虽然，两台主机之间相隔着一些网络，但网络层把每一个网络都看成一条链路或一条链路所组成的信道。因此两台主机之间通信的网络层协议应当包含如下内容：

（1）相互通信的主机的地址，即说明是哪个网络中的哪个主机。

（2）经过什么样的路径才能由源主机到达目的主机。有多条路径时，就有路径选择问题。

（3）在网络层的链路中传输，也有差错控制、流量控制等。

（4）运输层交来的是一个一个的数据报文段，是按照端对端的发送和接收能力划分的。这种划分不一定适合网络层划分。因此，在网络层还要继续对报文段进行划分，规定大小以及顺序等。

这些信息都要添加在重新划分的数据报中，在图 1.46 中用 H3（也可以写作 NH）表示。这种添加了 NT 的数据包被称为分组（packet）。

图 1.47 表明网络层与运输层的基本概念的不同。

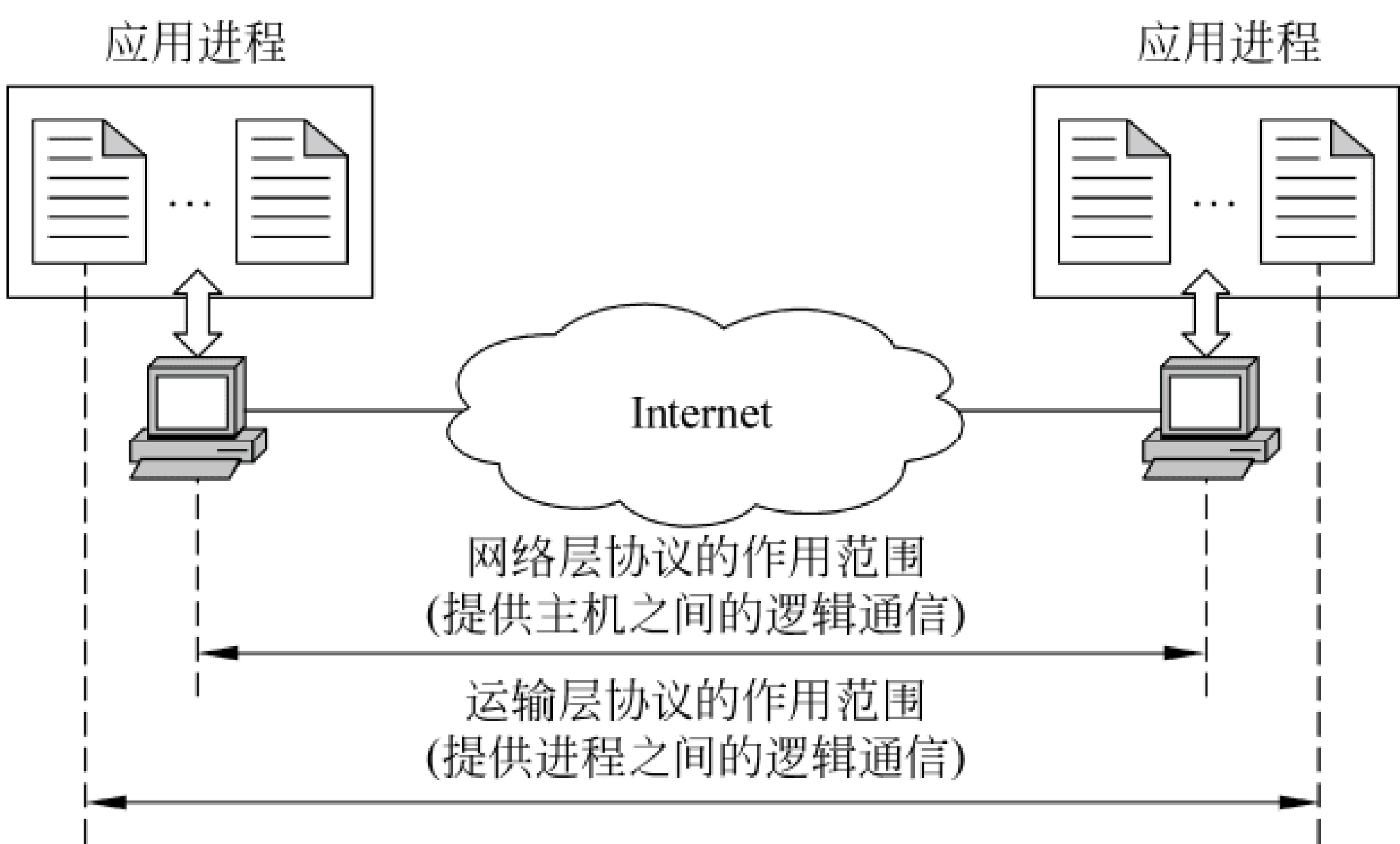


图 1.47　网络层与运输层的基本概念之不同

2．数据链路层

网络层把每一个网络都看成一条链路所进行的数据传输。为了支持网络层，数据链路层要解决在每一个网络中一条链路两端的通信问题。具体地说，数据链路层要解决如下问题。

（1）一个结点可能会是星形结构，即它连接多个了链路。因此首先要考虑传输是往哪个结点传输，为此要解决地址问题。这个地址用所连接的设备地址表示，称为物理地址，又称为 MAC（Media Access Control/Medium Access Control，媒体访问控制）地址。

（2）要保证在链路上可靠传送，就要关心传输中出现错误如何发现和处理。主要的技术是数据校验码、确认和反馈重发等。

（3）一个链路的两端的收发速率往往不同，如果发得快，收得慢，就会造成缓冲器溢出以及链路上的拥挤、阻塞，所以需要进行流量控制。

这些添加在网络层分组上的信息总称为 DH。进行封装后的数据报称为帧。H2（也可以写作 DH）称为帧头。

1．物理层

1）物理层的职责

图 1.48 为两个通信端点之间的通信模型。其中：

（1）数据终端设备（Data Terminal Equipment，DTE）为具有一定数据处理能力的发送、接收设备，如计算机或各种终端设备。



图 1.48　端到端通信模型

（2）数据通信设备（Data Communication Equipment，DCE）为通信接口设备，在 DTE 与通信网之间提供信号变换及编码功能，并负责建立、维护和释放物理连接，如波形变换器、基带传输器、调制解调器等。在现代的网络中，承担此功能的设备是网络适配器（network adapter），又称为通信适配器或网络接口卡（Network Interface Card，NIC），简称网卡。

2）物理层的性能

物理层性能具体表现为 DTE 与 DCE 之间的接口特性，它包括如下 4 个方面。

- 机械特性：形状、尺寸、引脚数等。
- 功能特性：各引脚功能等。
- 电气特性：转换电平、传输速率和距离等。
- 规程特性：信号工作的时序关系。

下面以最常用的 RJ-45 为例说明这些特性的作用。

（1）机械特性。图 1.49 给出了 RJ-45 的部分形状、尺寸和引脚，以及引脚间的举例。显然，如果另一个接插件不符合这个尺寸，就无法接插在一起。

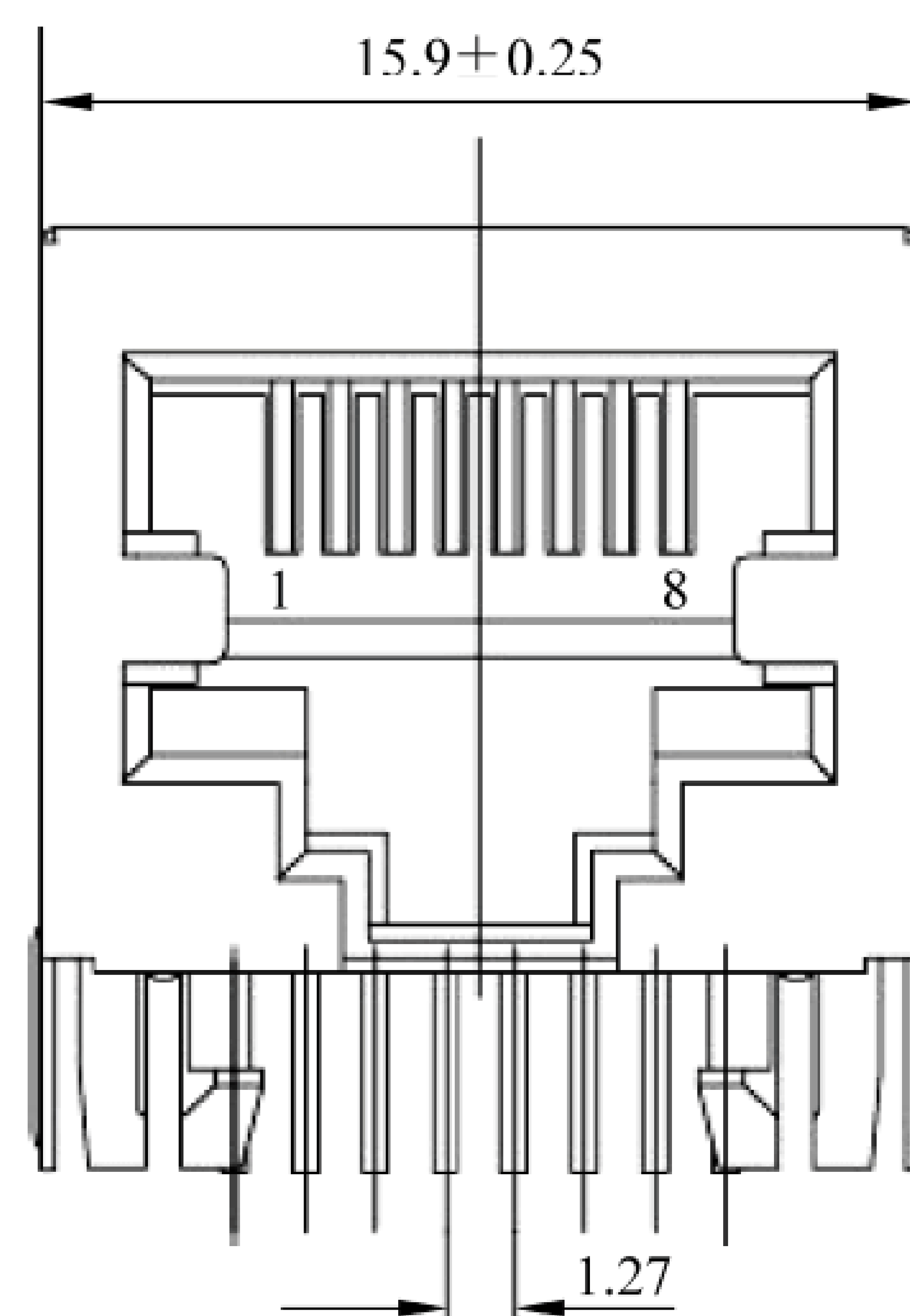


图 1.49　RJ-45 的部分机械特性

（2）功能特性。图 1.50 给出了 RJ-45 的两种接口定义。

表 1.7 为按照 TIA/EIA 标准定义的 RJ-45 的两种接口引脚定义。表 1.8 给出了这两种接口的用法。图 1.51 为交叉线的用法示意图。显然，不符合这些规则，连接后也无法正常工作。

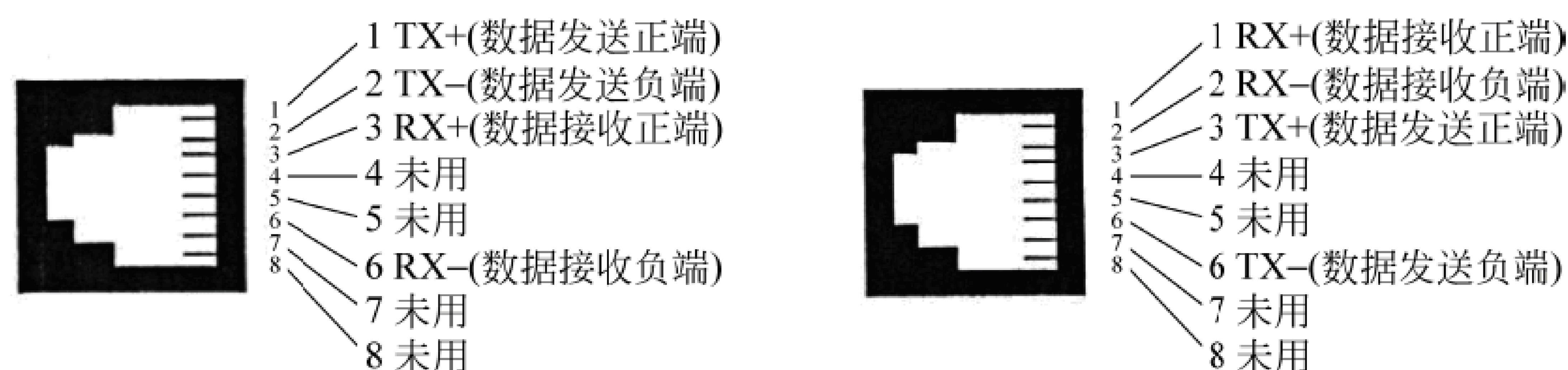


图 1.50　RJ-45 的两种接口功能定义

表 1.7　TIA/EIA 布线标准的两种线序的色线与脚位的对应关系

脚位	1	2	3	4	5	6	7	8
TIA/EIA568A	绿白	绿	橙白	蓝	蓝白	橙	棕白	棕
TIA/EIA568B	橙白	橙	绿白	蓝	蓝白	绿	棕白	棕

表 1.8　直通线、交叉线的排列线序和使用场合

线序	连接方式	使用场合
直通线	T568B - T568B T568A - T568A	在异种设备之间，如：计算机-集线器，计算机-交换机，路由器-集线器，路由器-交换机，集线器-集线器（UPLink 口），交换机-交换机（UPLink 口）
交叉线	T568B - T568A	在同种设备之间，如：计算机-计算机，路由器-路由器，计算机-路由器，集线器-集线器，交换机-交换机

（3）电气特性。如图 1.52 所示，为了屏蔽外界干扰，延长传输距离，网线采用两根线双绞在一起的线传输一个信号，以使两根线上感应的杂波信号基本相同但方向相反而抵消。所以网线转输过程中没有固定的 0 电平，而是采用两根线的中值当作“地”电平。只要两根线的电势差小于 1.6V 即可认为是 0；两根线的电势差大于 8V，就可确认为 1。

（4）规程特性。规程特性指多个信号间的时序关系。这种网线传输的信号非常简单，没有时序关系。

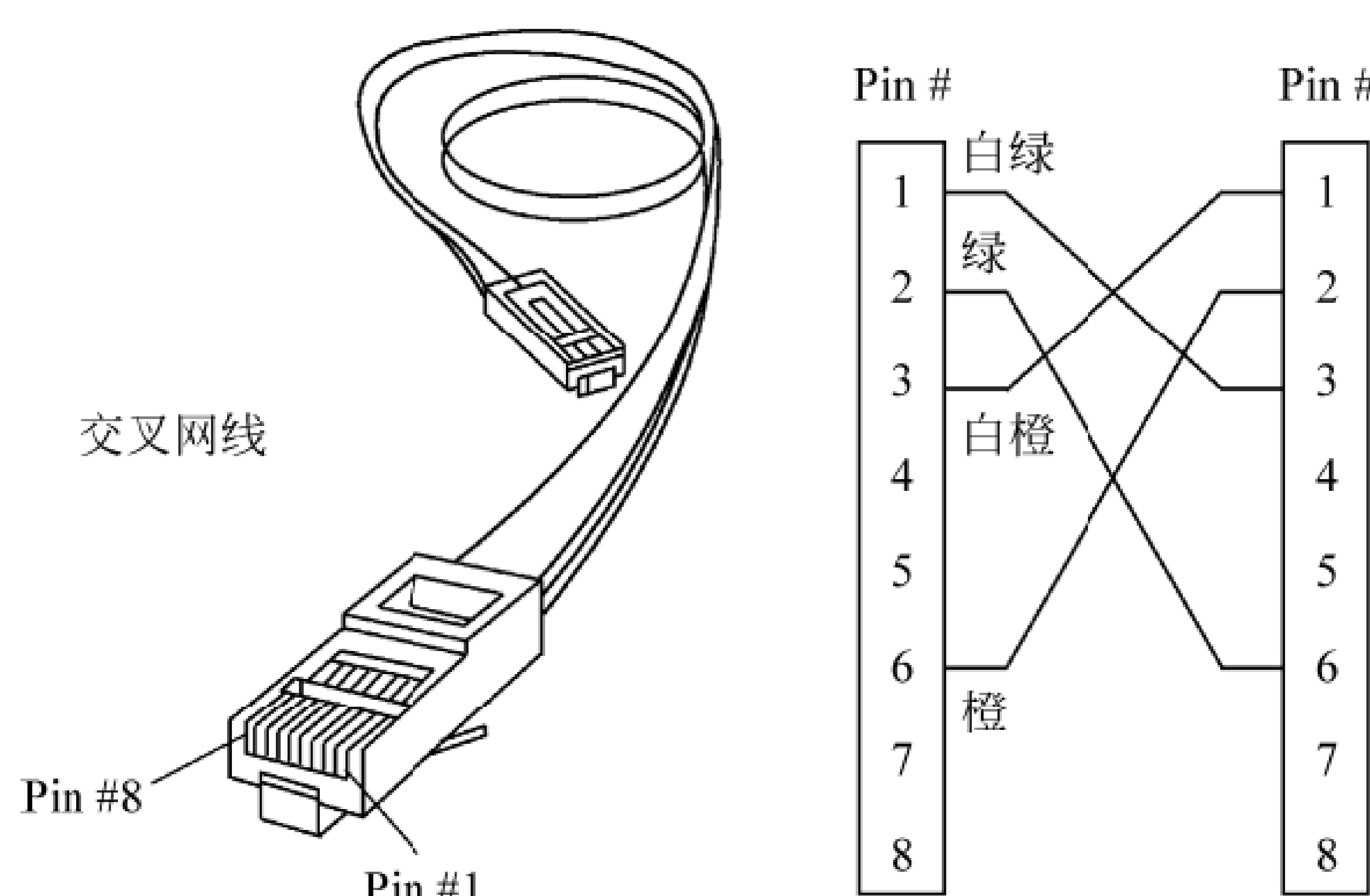


图 1.51　交叉网线（568A/568B）的连接示例

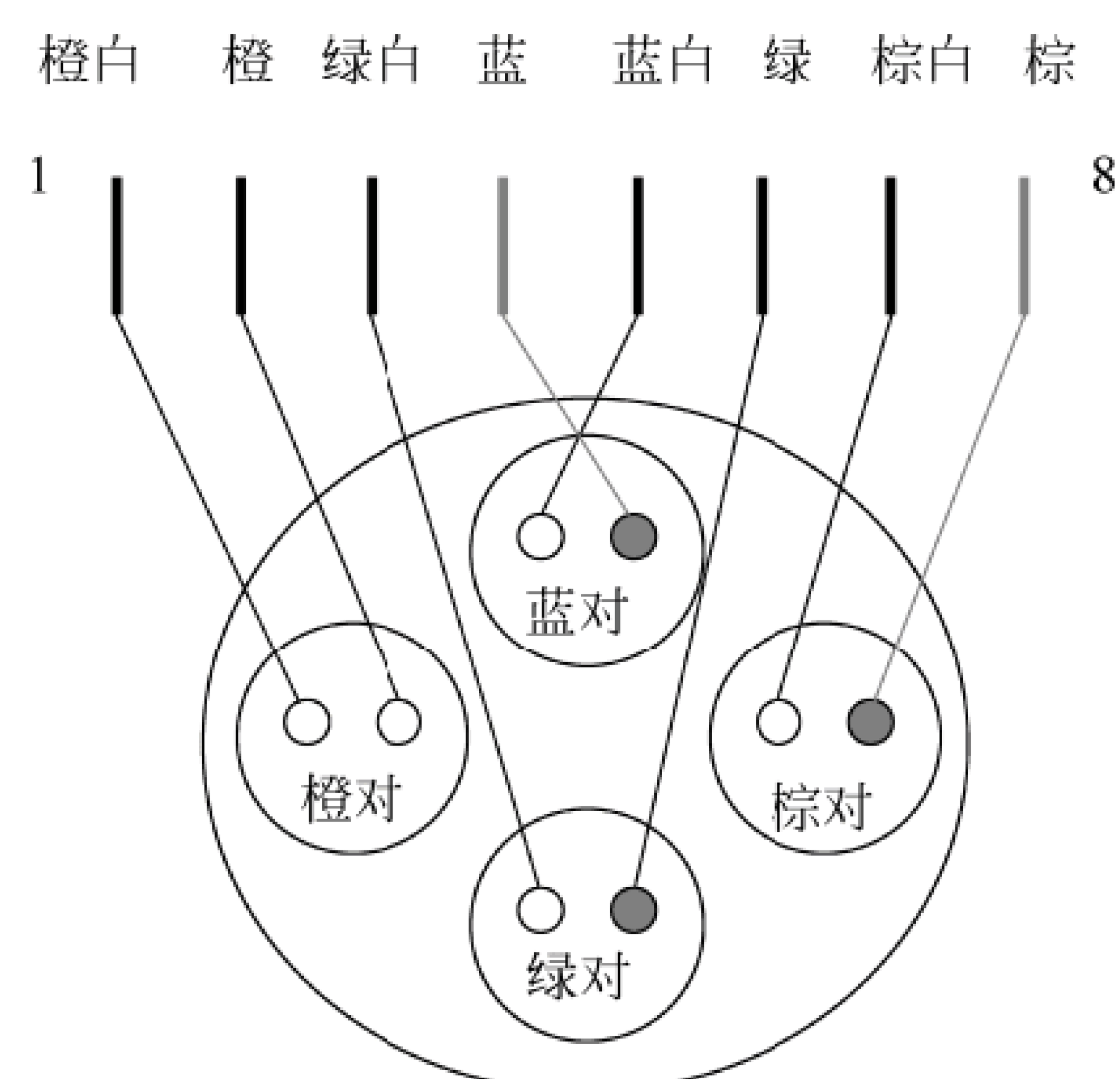


图 1.52　8 芯双绞线的扭绞规则

3）对于物理层性能的解释

上述特性决定了信道的下面一些参数：

（1）信道的频带宽度和极限容量。例如，10 100base tx RJ45 接口是常用的以太网接口，支持 10Mb/s 和 100Mb/s 自适应的网络连接速度。

（2）信道的交互方式是全双工方式，因为它具有收发两个信道。

（3）它是串行传送（数据只能一位一位地传送）。

OSI/RM 没有定义数据传输的物理介质，而是把所有实体的活动建立在了传输介质之上。这给计算机网络提供了一定的发展空间。

1.6　计算机网络工业标准：TCP/IP 和 IEEE 802

由于技术发展、历史、习惯、市场以及权势等因素的影响，在众多领域中存在多种技术标准并存的现象，其中信息处理领域尤为突出。在这些并存的技术标准中，每个子领域的标准往往都有两大类：一类称为法定标准，是由权威的标准制定不同机构所制定的标准；

另一类称为事实标准或工业标准，是由企业推行，实际具有一定市场份额的产品标准。在计算机网络领域，OSI/RM 就是一种法定标准，提供了一种框架，仅供参考。而事实标准是 TCP/IP 和 IEEE 802。

1.6.1 基于网络互联的 TCP/IP 网络体系结构

1. APRAnet 与 TCP/IP

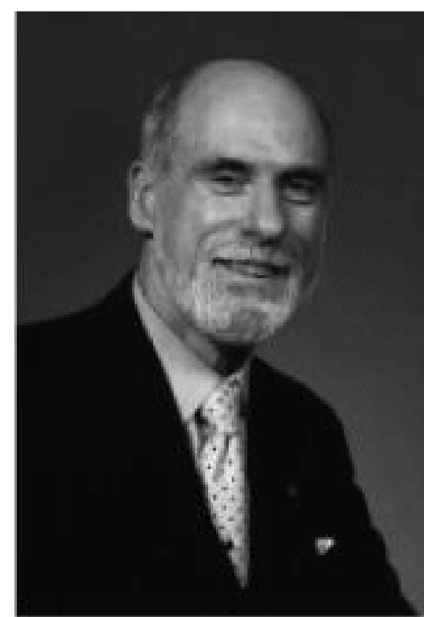
20 世纪 60 年代，ARPA（Advanced Research Projects Agency，美国国防部高级研究计划管理署）开始研究如何建立分散式指挥系统，以保证战争中部分指挥点被摧毁后其他点仍能正常工作。这项研究的主要内容是如何把分散在不同地点的异种计算机连接起来。1968 年时任 APRA 信息处理处处长的拉里 • 罗伯茨（Larry Roberts，图 1.53（a））提交了一份研究报告，提出构建 APRAnet 的设想。这个项目的团队很快形成，由罗伯茨提出网络思想设计网络布局，罗伯特 • 卡恩（Robert Elliot Kahn，1938 年 12 月 23 日—，图 1.53（b））设计阿帕网总体结构，温顿 • 瑟夫（Vinton G. Cerf，1943 年 6 月 23 日—，图 1.53（c））参与程序编写，还有众多的科学家、研究生参与研究、试验。他们选择了分布在洛杉矶的加利福尼亚州大学洛杉矶分校、加州大学圣巴巴拉分校、斯坦福大学、犹他州大学 4 所大学的 4 台不同型号的大型计算机进行联网实验。



(a) Larry Roberts



(b) Robert Elliot Kahn



(c)Vinton G. Cerf

图 1.53 为 APRAnet 做出巨大贡献的三位杰出人才

1969 年 9 月 APRAnet 开始运行。运行后发现，各个 IMP（Interface Message Processor，接口信息处理机）连接的时候，需要考虑用各计算机都认可的信号来打开通信管道，并在数据通过后关闭通道，否则这些 IMP 不会知道什么时候应该接收信号，什么时候该结束。这实际上就是通信协议的概念。于是卡恩和瑟夫开始开发一个称为 NCP（Network Control Protocol，网络控制协议）的软件，并于 1970 年 12 月开始使用。此时，ARPAnet 已初具雏形，遂开始向非军用部门开放，许多大学和商业部门开始接入。与此同时，美国的计算机网络热潮已显端倪，于是 DARPA 决定投入更大的力量，将研究重点放在网络互联上。他们把网络互联的核心工作分为两部分：一部分负责发现传输中的问题，一旦发现问题，就发出信号要求重新传输，直到所有数据安全正确地传输到目的地。这部分协议称为传输控制协议（Transmission Control Protocol/Internet Protocol，TCP/IP）；另一部分负责给主机规定地址，并能按照地址找到主机。这部分协议称为互联网协议或网际协议（Internet Protocol，IP）。

这两种协议合起来称为 TCP/IP。1973 年夏天，卡恩和瑟夫开发出了一个 NCP 的改进版本，这种协议可以屏蔽网络协议之间的不同。1974 年 12 月，卡恩和瑟夫的第一份 TCP 协议详细说明正式发表。到 1980 年前后，ARPAnet 上所有的主机都转向 TCP/IP 协议，随之也将 ARPAnet 称为 Internet 或 TCP/IP 网络。

瑟夫和卡恩的贡献打开了人们通向信息高速公路的大门，他们二人也一起获得了包括图灵奖、美国国家技术奖、美国总统自由勋章等在内的众多荣誉。

1992 年 Internet 被交给国际性组织 ISOC（Internet Society，因特网协会）管辖。其中，技术方面由 IAB（Internet Architecture Board，因特网体系结构委员会）负责。

2．TCP/IP 模型

一开始 TCP 与 IP 这两个协议只有分工，还没有层次组织的思想，而且 ARPAnet 的应用也很简单。后来，Internet 的应用急剧增加，所连接的网络迅速膨胀，人们开始考虑 IP 与具体网络之间的接口问题，也开始考虑应用协议问题。OSI/RM 提出后，它开始向 OSI/RM 靠拢，用层次结构对其所有协议进行划分，加给它一个层次形态。所以，对于 Internet 体系的层次的划分并不是非常严格，也不完全，后来又打补丁、加套接层，形成图 1.54 中用虚线表示与 OSI/RM 的对应关系。它的 4 层结构是应用层、传输控制层、网际层和网络接口层。



图 1.54　TCP/IP 网络模型及其与 OSI/RM 的对应关系

在 TCP/IP 网络模型中，应用层（Application Layer）是与应用程序的接口，网络访问层（Network Access Layer）是与具体网络的接口。但是，它们只是提供了一个框架，没有详细描述，这给后来的技术发展留下两个空间。关于它们的被填充情况将在第 3 章和第 4 章介绍。TCP/IP 的核心和贡献就在运输层（Transport Layer）和网际层（Internet Layer）。

1）传输层

TCP/IP 的传输层为了向应用层提供透明传输服务，它要将应用层的数据报文分割成数据段或报文段，并根据应用的特点分别按照传输控制协议（Transmission Control Protocol，TCP）和用户数据报协议（User Datagram Protocol，UDP）进行端对端地传输。TCP 是面向连接的协议，它提供可靠的报文传输和对上层应用的连接服务。为此，除了基本的数据传输外，它还有可靠性保证、流量控制、多路复用、优先权和安全性控制等功能。UDP 是面向无连接的不可靠传输的协议，主要用于不需要 TCP 的排序和流量控制等功能的应用程序。

2）网际层

TCP/IP 的网际层为了透明地支持运输层的虚电路和数据报，会将运输层的数据段或报文段进一步分割成适合所有网络传输的分组，并使分组能独立地传向目标主机。为此，在 IP（Internet Protocol，网际协议）中定义了 IP 地址（也称主机地址或网络地址）和路由等协议。目前广泛使用的 IPv4 使用 32b 的 IP 地址，每个 IP 地址分为网络地址和主机地址两部分，通常用 4 个点分的十进制数表示，如 202.113.240.32。新的 IP 版本 IPv6 则用 128b 表示 IP 地址，以满足日益增长的联网需求。

关于 TCP/UDP 和 IP 的细节将在第 3 章介绍。

1.6.2　IEEE 802 模型

几乎在 Interent 迅速发展的同时，局域网也在迅速发展。IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师协会）于 1980 年 2 月成立了 LMSC（LAN /MAN Standards Committee，局域网/城域网标准委员会)，简称 IEEE 802 委员会，专门从事局域网/城域网的标准化工作，制定出了一系列标准，统称为 IEEE 802 标准，这些标准的模型称为 IEEE 802 模型。

IEEE 802 模型参考了 OSI 参考模型，但主要包含了 OSI 参考模型的低两层：物理层和数据链路层，如图 1.55 所示。

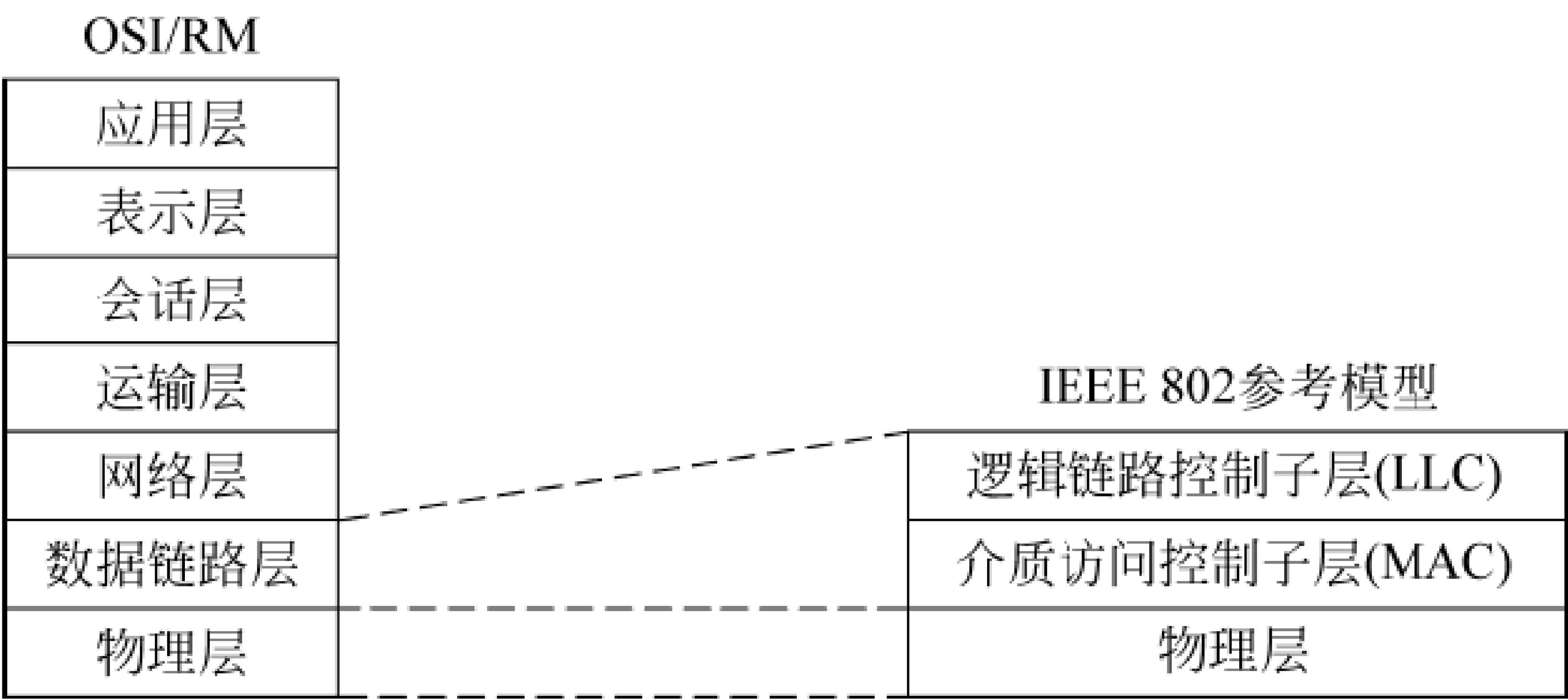


图 1.55　IEEE 802 模型及其与 OSI/RM 的对应关系

1．物理层

物理层主要规定了机械、电气、功能和规程等方面的特性，以确保在通信信道上二进制位信号的正确传输和接收，内容包括物理介质、物理介质连接设备（Physical Medium Attachment，PMA）、连接单元接口（Attachment Unit Interface，AUI）和物理信号（Physical Signaling，PS）格式，以及对于同步、编码、译码、拓扑结构和传输速率的要求。

2．数据链路层

局域网的拓扑结构比较简单且多个站点共享传输信道。这样就需要解决信道的访问控制（即接入方式）问题，即采用什么样的控制方式进行信道资源的分配。然而，信道的访问控制方式与传输介质的关系密切。为此，局域网也将数据链路层分为两个子层。

1）传输介质访问控制（Medium Access Control，MAC）子层

介质访问控制 MAC 子层是与介质有关的子层，负责解决与媒体接入有关的问题和在物

理层的基础上进行无差错的通信。MAC 子层的主要功能是：发送时将上层交下来的数据封装成帧进行发送，接收时对帧进行拆卸，将数据交给上层；实现和维护 MAC 协议；进行比特差错检查与寻址。

为了寻址，它定义了长度为 48b（6B）的 MAC 地址，对链路层的设备进行标识。所以 MAC 地址也称物理地址、硬件地址或链路地址，通常用 6 组杠分十六进制数表示，每组两个十六进制码，表示一个字节，如 00-58-CE-07-0C。

2）与介质无关的子层——逻辑链路控制（Logical Link Control，LLC）子层

该层与具体局域网使用的介质访问方式无关，其主要功能是：建立和释放数据链路层的逻辑连接；进行帧的拆装、帧顺序的控制、差错控制以及流量控制；提供与上层的接口（即服务访问点）。

1.6.3　基于 TCP/IP＋ 物理网的流行网络体系结构

随着通信技术的进步和计算机网络技术的发展，局域网的传输距离不断扩大，使得它与城域网之间的界线日趋模糊。因此，IEEE 802 已经不再局限于局域网，而扩大到所有物理网。与此同时，由于 TCP/IP 的普及，使得现在的计算机网络实际上都遵循了如图 1.56 所示的体系结构。图中还给出了在这个体系中数据传输过程的封装过程。本书将在后面的章节中按照这个体系介绍计算机网络的原理和引用。

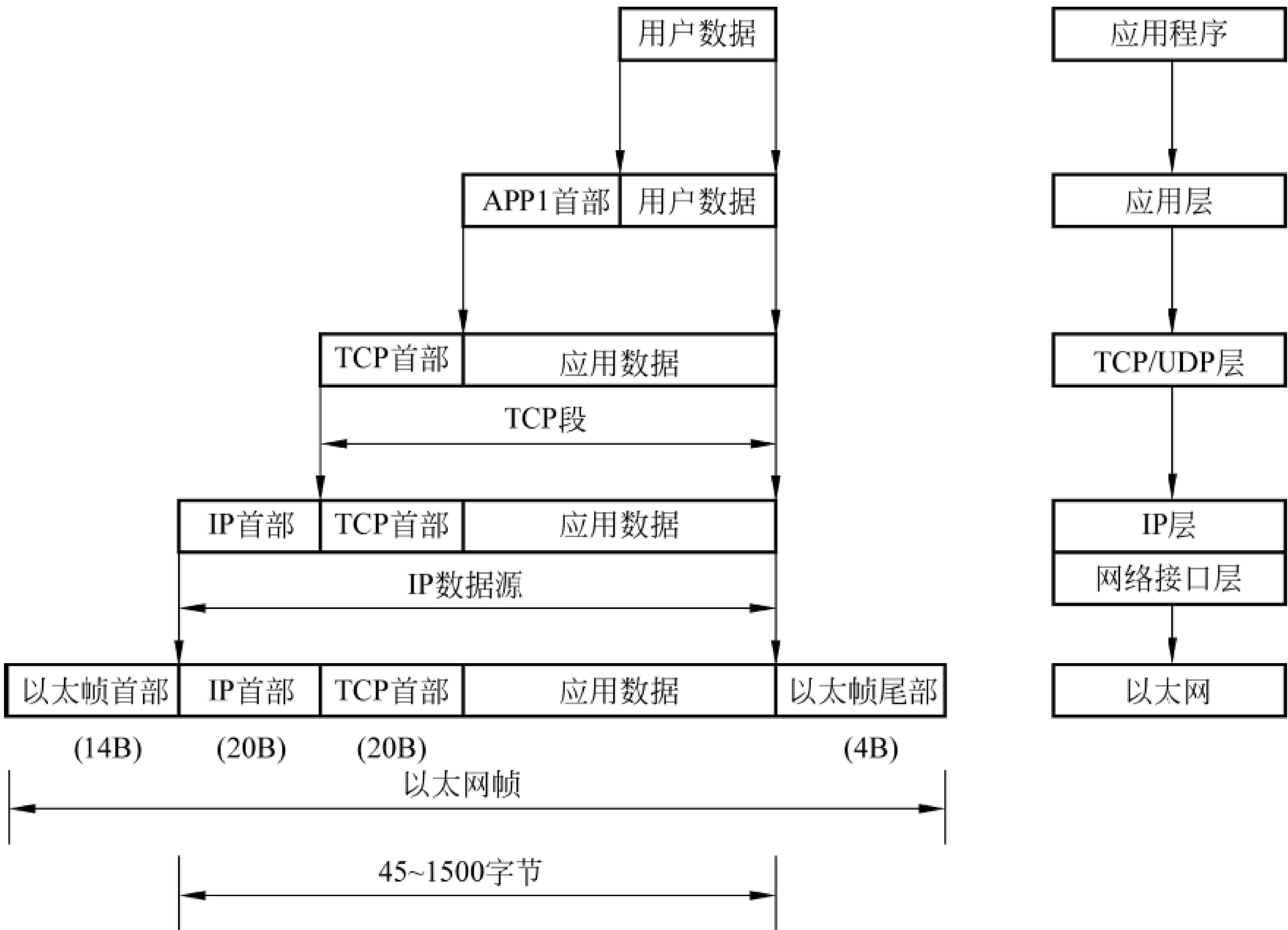


图 1.56　TCP/IP＋ 以太网的流行五层网络体系

图 1.56 中的“以太网（Ethernet）”是指由 Xerox 公司创建并由 Xerox、Intel 和 DEC 公司联合开发的基带局域网规范。现在它已经成为了当今物理网采用的最通用的通信协议标准。

实验 1　RJ–45 网线制作

一、实验内容

制作双绞线的 RJ-45 网线。

二、材料准备

（1）非屏蔽 5 类双绞线 2～3m。
（2）4 个 RJ-45 接头，如图 1.57 所示。
（3）4 个 RJ-45 护套。

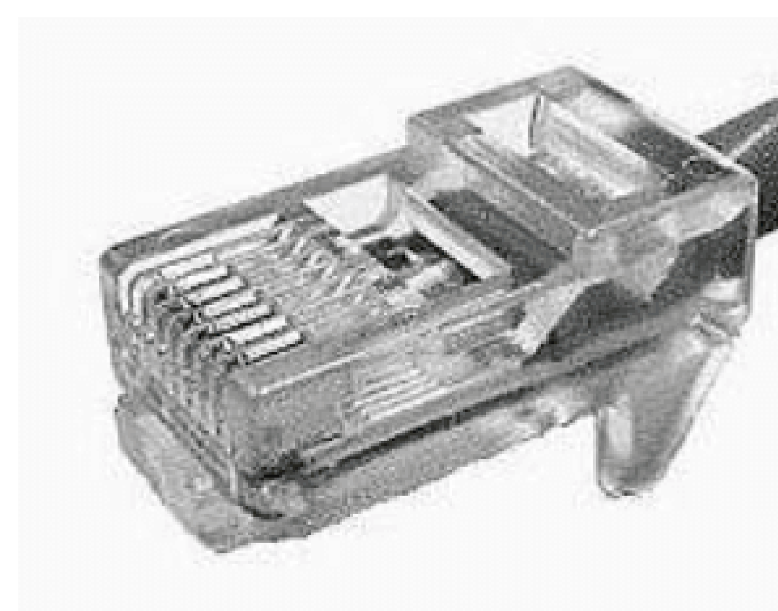


图 1.57　水晶头

三、工具准备

（1）RJ-45 压线/剥线钳一把，如图 1.58 所示。
（2）RJ-45 测线仪一个，如图 1.59 所示。
（3）剪线钳一把。



图 1.58　RJ-45 压线/剥线钳



图 1.59　一款简单的测线器（通断仪）

四、预备知识

1. EIA/TIA-568 标准

随着计算机网络的发展，计算机与通信系统之间的连接越来越成为非常普通的工程项目。但是，直到 20 世纪 80 年代初，在建筑行业中还没有关于这方面的标准。1985 年美国 CCIA（Computer Communications Industry Association，计算机通信协会）就请 EIA（Electronic Industries Association 美国电子工业协会）制定出有关标准。1991 年 7 月，第一个版本的标准出现，这就是 EIA/TIA-568。现在的网线制作都要遵照这个标准。

2. 制作网线用的双绞线

按照 EIA/TIA-568 标准，双绞线按电气特性区分有：三类、四类、五类线。网络中最常用的是三类线和五类线，目前已有六类以上线。第三类双绞线在 LAN 中常用作为 10Mbps 以太网的数据与话音传输，符合 IEEE 802.3 10Base-T 的标准。第五类双绞线目前占有最大的 LAN 市场，最高速率可达 100Mbps，符合 IEEE 802.3 100Base-T 的标准。如图 1.52 所示，

它们都是按照蓝-蓝白（BL,W-BL）、橙白-橙（W-O,O）、绿白-绿（W-G,G）、棕白-棕（W-R,R）分别扭绞的 4 对线，分别称为蓝对线（Pair1）、橙对线（Pair2）、绿对线（Pair3）、棕对线（Pair4）。

3. RJ-45 接头

RJ-45 水晶头由金属片和塑料构成。双绞线的两端要连接到 RJ-45 水晶头，才可以连接网络设备。将 RJ-45 与双绞线连接时也要遵照 EIA/TIA-568 标准。为此需要搞清其引脚序号。当金属片面对我们的时候，从左至右引脚序号是 1～8，这序号在做网络联线时非常重要，不能搞错，目的是保证线缆接头布局的对称性。

五、参考步骤

（1）根据设备之间的距离，或是设备与配线架之间的距离，用剪线钳剪一段双绞线，最大长度为 3m。

（2）将 RJ-45 护套自一端套入双绞线。

（3）将电缆护套自一端剥去，裸露的导线长度不少于 20mm，电缆护套长度不少于 13mm，如图 1.60 所示，并将电缆固定。

（4）把裸露部分的 4 组导线分开，使其线对顺序依次为 1 和 2（白绿/绿）、3 和 6（白橙/橙）、4 和 5（白蓝/蓝）、7 和 8（白棕/棕）。

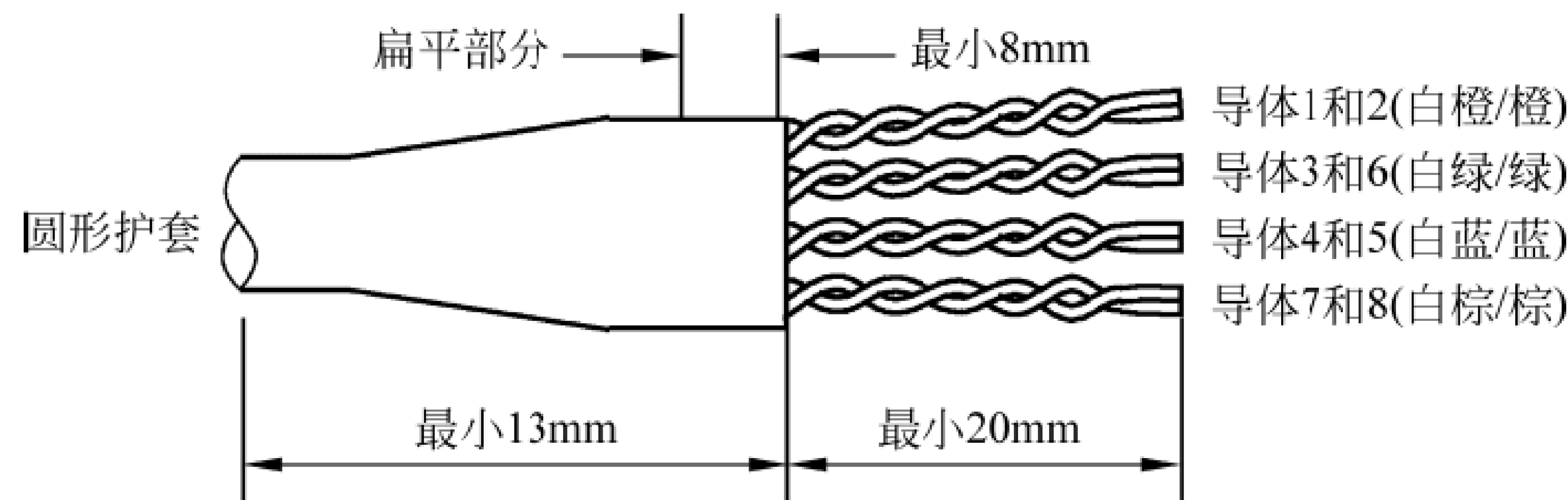


图 1.60　电缆护套剥除长度和要求

（5）将每对线解开绞合，每条线都互相平行。根据所选用的布线设计（EIA 568B，直通电缆）布置好导线的正确顺序，按正确的定位顺序排列（绿白、绿、橙白、蓝、蓝白、橙、棕白、棕），其中导线 6 跨过导线 4 和导线 5。在排好导线后，再将它们的正确顺序检查两遍。要求护套内的导线交叉长度不发生变化，不要松开。

（6）用剪线钳在线缆护套端头以外 14mm 处整齐地切断。确保导线端头截面的平整，不应有毛刷或不齐现象，以免影响性能。整理好的导线长度应为 14mm，从导线端头开始至少 10+1mm 的一段长度，导线之间不应有交叉现象，导线 6 跨越导线 4 和导线 5 的地方离护套的距离不应超过 4mm，如图 1.61 所示。

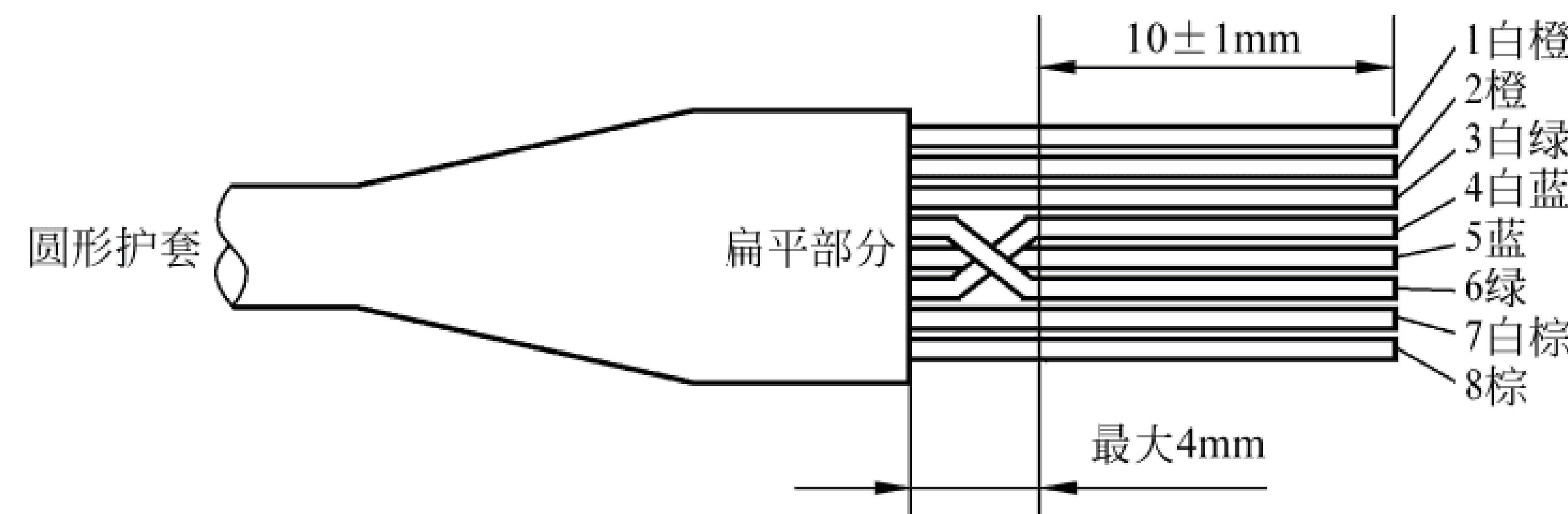


图 1.61　线对排列

（7）将整理好的电缆导线插入RJ-45接头中，导线的端头一直伸到RJ-45接头的前端最底部为止。电缆护套的扁平部分应从插头后端插伸到超过预张力释放压块下，电缆护套应伸出插头后端至少6mm（注意：导线插入RJ-45插头时，含有金属片的一面向上，其顺序为从左到右，其顺序应与电缆导线顺序一致）。

（8）检查电缆每条导线的顺序是否正确，每条导线是否已到达R-45接头的最底部（此时从RJ-45接头的另一端应当看得到导线头）。

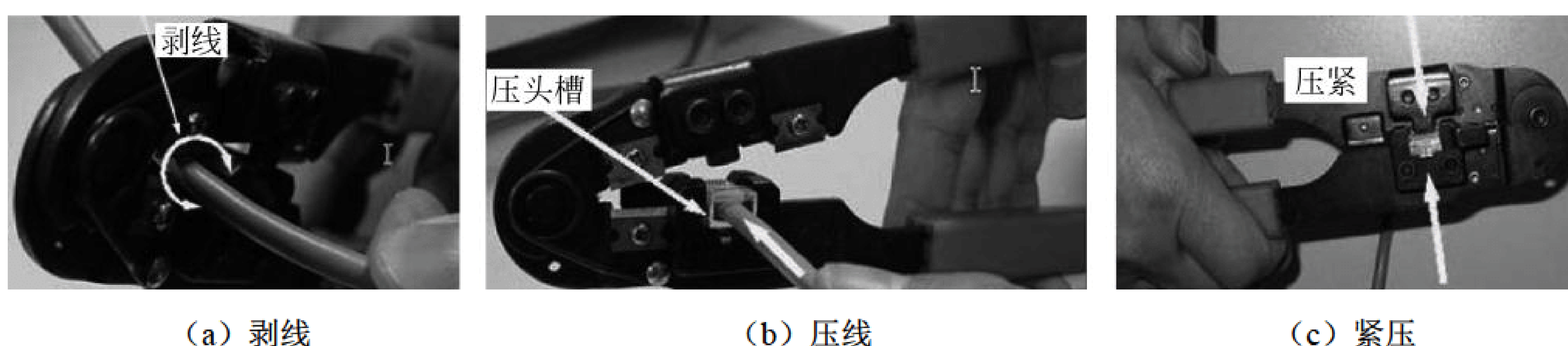
（9）将RJ-45接头插入压线/剥线钳的RJ-45插座，然后用力压紧，使RJ-45接头紧咬在双绞线上，再次测量导线和护套的长度，以确定它们是否符合规定的几何尺寸要求。

（10）将RJ-45护套套到RJ-45接头上，以确保其性能与美观。

（11）重复以上步骤制作双绞线的另一端RJ-45接头。注意，每一条细线的顺序必须与另一端相同。

图1.62为在上述过程中，RJ-45压线/剥线钳的使用方法。

依照上述方法分别做一根直通网线和一根交叉网线。



（a）剥线　　（b）压线　　（c）紧压

图1.62　RJ-45压线/剥线钳的使用方法

六、测试

网线制作好后，应当首先进行连通性测试。连通性测试可以使用仪器仪表进行。最简单的常用仪表是普通万用表（通断仪），或者是在网络布线中常用的测线器（cable tester）。好的测线器（通断仪）将显示出线缆的问题以及RJ-45头是否打（压接）好。

该工具是由主副两部分组成。测试线缆时，应将一根线缆的两端分别插入主副测试仪（通断仪）的插座中，然后打开电源。对于直通型双绞线，正确时，两端的8个信号灯会顺序地跳亮；对于交叉线，主测试仪端信号灯按1—2—3—4—5—6—7—8的顺序亮灯时，副测试仪中信号灯会按1—3—2—4—5—6—7—8（3—6—1—4—5—2—7—8）的顺序亮灯。若不是上述情况，则表明有错。

七、分析与讨论

（1）有交叉的网线与无交叉的网线各适合在何种情况下使用？

（2）网线制作好后就可以直接使用吗？

习　题　1

一、选择题

1. 下列【　　】最好地描述了基带信号。
   A. 通过同一通道传输的多重信号　　B. 通道上的频率范围通常要进行划分的信号
   C. 是多进制方波形式　　D. 以其原始的状态传输的信号
2. 波特率等于【　　】。
   A. 每秒传输的比特　　B. 每秒传输的周期数
   C. 每秒钟发生的信号变化的次数　　D. 每秒传输的字节数
3. 若网络形状是由结点与结点首尾相连而形成的一个闭合环路，则称这种拓扑结构为【　　】。
   A. 星形拓扑　　B. 总线型拓扑　　C. 环形拓扑　　D. 树形拓扑
4. 一座大楼内的计算机网络系统，属于【　　】。
   A. PAN　　B. LAN　　C. MAN　　D. WAN
5. 网络协议的三要素为【　　】。
   A. 数据格式、编码、信号电平　　B. 数据格式、控制信息、速度匹配
   C. 语法、语义、时序　　D. 编码、控制信息、同步
6. 通信系统必须具备的3个基本要素是【　　】。
   A. 终端、电缆、计算机　　B. 信号发生器、通信线路、信号接收设备
   C. 信源、通信信道、信宿　　D. 终端、通信设施、接收设备
7. 下列【　　】最好地描述了基带信号。
   A. 通过同一通道传输多重信号　　B. 对通道上的频率范围通常要进行划分
   C. 是多进制方波形式　　D. 信号以其原始的状态传输
8. 误码率是通信系统中衡量系统可靠性的指标。在计算机网络中，对误码率的要求是低于【　　】。
   A. 10^{-4}　　B. 10^{-6}　　C. 10^{-9}　　D. 10^{-2}
9. 采用全双工通信方式，数据传输【　　】。
   A. 可以在两个方向上同时传输　　B. 只能在一个方向上传输
   C. 可在两个方向上传输，但不能同时　　D. 以上均不对
10. 下列编码中，自含时钟的是【　　】。
    A. 单极性不归零码　　B. 单极性归零码
    C. 曼彻斯特编码　　D. 双极性归零码
11. 同步和异步两种通信方式，传送效率【　　】。
    A. 同步方式更高　　B. 异步方式更高
    C. 两种方式相同　　D. 无法比较
12. 调制解调器的主要功能是【　　】。
    A. 模拟信号的放大　　B. 数字信号的整形
    C. 模拟信号与数字信号的转换　　D. 数字信号的编码

13．发送端将数字信号变换另一种数字信号的过程叫作【　　】。

A．编码　　B．解码　　C．调制　　D．解调

14．采用曼彻斯特编码，100Mbps传输速率所需要的调制速率为【　　】。

A. 200MBaud　　B. 400MBaud　　C. 50MBaud　　D. 100MBaud

15. 将一条物理信道按时间分成若干个时间片轮换地给多个信号使用，每一个时间片由其中一个信号占用，可以在一条物理信道上传输多个数字信号，这是【　　】复用。

A．频分多路　　B．时分多路　　C．波分多路　　D．空分多路

16．T1载波的数据传输率为【　　】。

A. 1Mbps　　B. 10Mbps　　C. 2.048Mbps　　D. 1.544Mbps

17．下列差错校验方法中，【　　】的检错能力最强。

A．奇校验　　B．偶校验　　C．方阵校验　　D．循环冗余校验

18．网络体系结构可以定义为【　　】。

A．一种计算机网络的实现

B．建立和使用通信硬件和软件的一套规则和规范

C．执行计算机数据处理的软件模块

D．由ISO制定的一个标准

19．下列功能中，不是OSI物理层功能的是【　　】。

A．定义硬件接口的电气特性　　B．定义硬件接口的机密特性

C．定义硬件接口的功能特性　　D．定义硬件接口的机械特性

20．用双绞线连接以下设备时，需要使用交叉线的场合是【　　】。

A．计算机网卡与计算机连接　　B．计算机网卡与交换机连接

C．两个集线器上专用级联口级联时　　D．两台计算机通过网卡字节连接时

21．在OSI七层结构模型中，处于数据链路层与运输层之间的是【　　】。

A．物理层　　B．网络层　　C．会话层　　D．表示层

22．在下列功能中，【　　】最好地描述了OSI模型的数据链路层。

A．保证数据正确的顺序、无错和完整　　B．提供用户与网络的接口

C．处理信号通过介质的传输　　D．控制报文通过网络的路由选择

23. 传输层的作用不包括下列【　　】。

A．建立运输站　　B．拆除运输站

C．把信息组装成包　　D．负责数据传输

24．下列功能中，属于表示层提供的功能的是【　　】。

A．交互管理　　B．透明传输　　C．死锁处理　　D．加密、解密

25．网络层、数据链路层和物理层互联设备转发或传输的数据单元分别是【　　】。

A．报文、帧和比特　　B．分组、报文和比特

C．分组、帧和比特　　D．数据块、分组和比特

26. 运输层、数据链路层和物理层传输的数据单元分别是【　　】。

A．报文段、帧和比特　　B．分组、报文段和比特

C．报文、帧和比特　　D．数据块、分组和比特

27．TCP/IP协议的含义是【　　】。

A．局域网传输协议　　　　B．拨号入网传输协议

C．传输控制协议/网际协议　　　　D．OSI协议集

28．用来标识网络设备位置的MAC地址是由【　　】二进制数组成的。

A．16位　　B．24位　　C．32位　　D．48位

二、填空题

1．传输速率单位bps代表________。

2．计算机网络系统是由负责________的通信子网和负责信息处理的________子网组成的。

3．在OSI中，实现差错控制和流量控制的功能层次是________。

4．在信道上传输的信号分为两大类：________和________。

5．允许信号同时在两个方向上流动的数据传输方式叫作________。

6．常用的多路复用技术为________、________、________和波分多路复用。

7．在反馈重发差错控制机制中，连续工作方式又分为________和________。

8．将模拟信号转换成数字信号的具体步骤有________、________和量化。

9．数字信号转换成模拟信号的方法有________、________和________。

10．DTE与DCE间的物理接口特性是指________、电气特性、________和规程特性。

11．填写下表，完成双绞线网线跳接线线序标准。

	1	2	3	4	5	6	7	8
一端线序	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕
另一端线序								

12．可以将TCP/IP看成一个四层结构，其从下往上分别是________、________、________和________。

13．IEEE的局域网模型包括三层次(含子网)，分别是________、________、________。

三、简答题

1．什么是计算机网络？计算机网络有哪些功能？

2．计算机网络的拓扑结构主要有哪些？各有什么特点？

3．什么是网络协议?协议的三要素是什么?

4．什么是信道？按不同角度信道可以分成哪些类？

5．数据、信息、信号有什么不同？

6．什么是基带？什么是基带信号？什么是基带传输？

7．什么是串行通信？什么是并行通信？它们各有什么特点？

8．举例说明单工、半双工和双工通信的特点。

9．多路复用有哪些形式？各有什么特点？

10．对一个4kHz的无噪声信道每0.1ms采样一次，可以得到的最大传输速率有多少？

11．在50kHz的信道上，要传输T1信号，需要的信噪比最少要多大？

12．有一信道，频率范围为60～108kHz。假定每路信号的带宽为3.2kHz，各路信号间的防护间隔为

0.8kHz，若采用频分多路复用，最多可以同时传输几路信号？

13．什么是同步传输和异步传输？

14．为什么要进行差错控制？有哪些原因会造成传输出错？

15．请简述CRC校验原理。

16. 已知CRC生成多项式为$G(x) = x^4 + x + 1$，设要传送的码字为10110（从左到右发送），试计算校验码。

17. 为什么数据链路层协议要把CRC放在帧的尾部？

18. 一个4kHz的信道，传播延迟为20ms，为了使停-等协议至少有50%的效率，帧的大小应当在什么范围内？

19．滑动窗口协议有哪些作用？各是如何实现的？

20．什么是数据交换？

21．电路交换、报文存储转发交换和分组交换各有什么特点？

22．OSI/RM分为哪些层次？各层的主要功能是什么？

23．ISO在制定OSI/RM时，对于层次划分采用了哪些原则？

24．比较TCP/IP参考模型与OSI参考模型的异同。

25．什么是MAC地址？其作用是什么？

第 2 章　计算机网络组成

计算机网络是一种复杂的系统。但是，归纳起来它主要由计算机、传输介质、协议、网络操作系统和网络管理软件组成。一般说来，低层协议由通信控制处理器（中继器、交换机、路由器和网卡）实现，高层协议由网络操作系统和协议软件实现。这样，组成计算机网络的元素就可以分为三类：传输介质、通信控制处理器和网络软件。

2.1　传 输 介 质

传输介质是网络中信息传输的载体，也是网络通信的物质基础之一。传输介质的性能对传输速率、通信距离、可连接的网络结点数目、数据传输的可靠性等均产生很大的影响。因此，必须根据不同的通信要求，合理地选择传输介质。目前，常用的传输介质主要分为两种，即有线传输介质和无线传输介质。其中有线传输介质有双绞线、同轴电缆、光纤和电力线路等；而无线传输介质则有卫星、微波、蓝牙、激光、红外线和可见光等。包括：具体用什么介质，与网络要求的性能，特别是带宽有关。表 2.1 对其中常用的几种进行了比较说明。

表 2.1　几种传输介质的性能比较

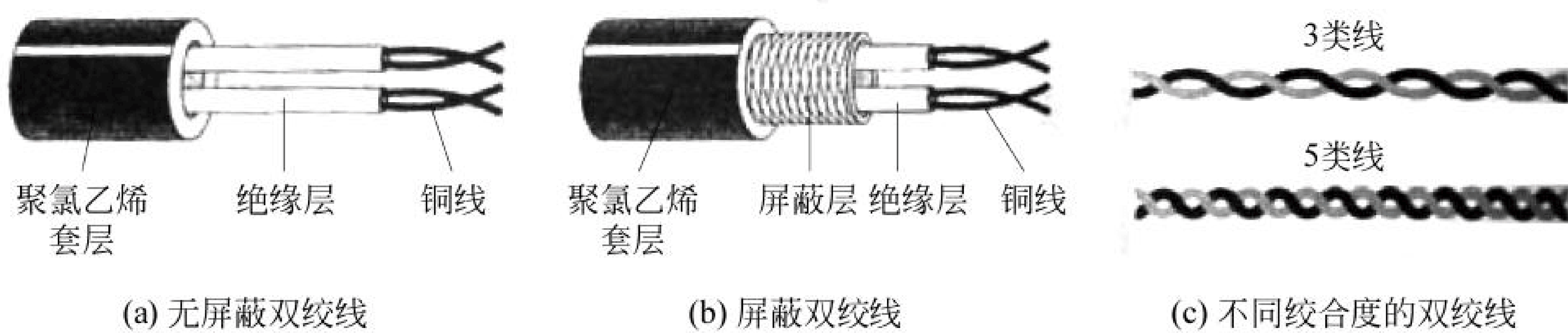
性　　能	双绞线	同轴电缆（基带）	同轴电缆（宽带）	光纤	地面微波	卫星
最大传输距离（km）	<0.3	<2.5	<100	100	40～50	不受限制
抗强电干扰性	较差	高	高	极高	差	差
安装难易程度	易	中	中	较难	易	易
布局多样性	好	较好	较好	中	好	好
保密性	一般	好	好	极好	差	差
经济性	低	较低	较低	较高	中	较高
时延	小	小	小	小	小	大

2.1.1　有线传输介质

1．双绞线

双绞线（Twisted Pair wire，TP）是最常用的一种传输介质。一对双绞线一般由两根 22～26 号绝缘铜导线相互缠绕而成。把一对或多对双绞线放在一个绝缘套管中便成了双绞线电缆。与其他传输介质相比，双绞线在传输距离、信道宽度、数据传输速度等方面均受到一定限制，但价格较为低廉。目前，双绞线可分为非屏蔽双绞线（Unshielded Twisted Pair，UTP）和屏蔽双绞线（Shielded Twisted Pair，STP），它们的结构分别如图 2.1（a）和（b）

所示。把两根绝缘的铜导线按一定密度互相绞在一起的目的是降低信号干扰的程度，一个外界干扰信号在两根一来一往绞合在一起的导线中，在理想状态下将互相抵消。抵消的程度与绞合的程度有关。如图 2.1（c）所示，5 类线的绞合程度比 3 类线高，所以抗干扰性就好。



(a) 无屏蔽双绞线　(b) 屏蔽双绞线　(c) 不同绞合度的双绞线

图 2.1　双绞线电缆

双绞线的性能参数包括衰减（attenuation）、近端串扰（NEXT）损耗、衰减串扰比（ACR）或信噪比（Signal-Noice Ratio，SNR）、阻抗特性、分布电容、直流电阻等。这些都影响到传输带宽和传输距离。如表 2.2 所示为各类铜质 UTP 的参数。

表 2.2　常用绞合线的带宽和应用

常用绞合线类别	传输带宽（100m 时）	应　用　说　明
3 类（Category Ⅲ）	16Mbps	低速网络与语音传输
4 类（Category Ⅳ）	20Mbps	短距离 10BASE-T 网络与语音传输
5 类（Category Ⅴ）	100Mbps	加了绕线密度，用于语音传输和 10BASE-T 网络，某些 100BASE-T
CAT 5E	100Mbps	衰减小，串扰少，具有更高的衰减与串扰的比值（ACR）和信噪比（Structural Return Loss）、更小的时延误差，用于 100BASE-T 及某些 1000BASE-T
6 类（E 类）（Category Ⅵ）	250Mbps	改善了串扰以及回波损耗性能，用于 1000BASE-T。永久链路的长度不能超过 90m，信道长度不能超过 100m
7 类（F 类）（Category Ⅶ）	600Mbps	只使用 STP，可用于 10Gbps 以太网

2．同轴电缆

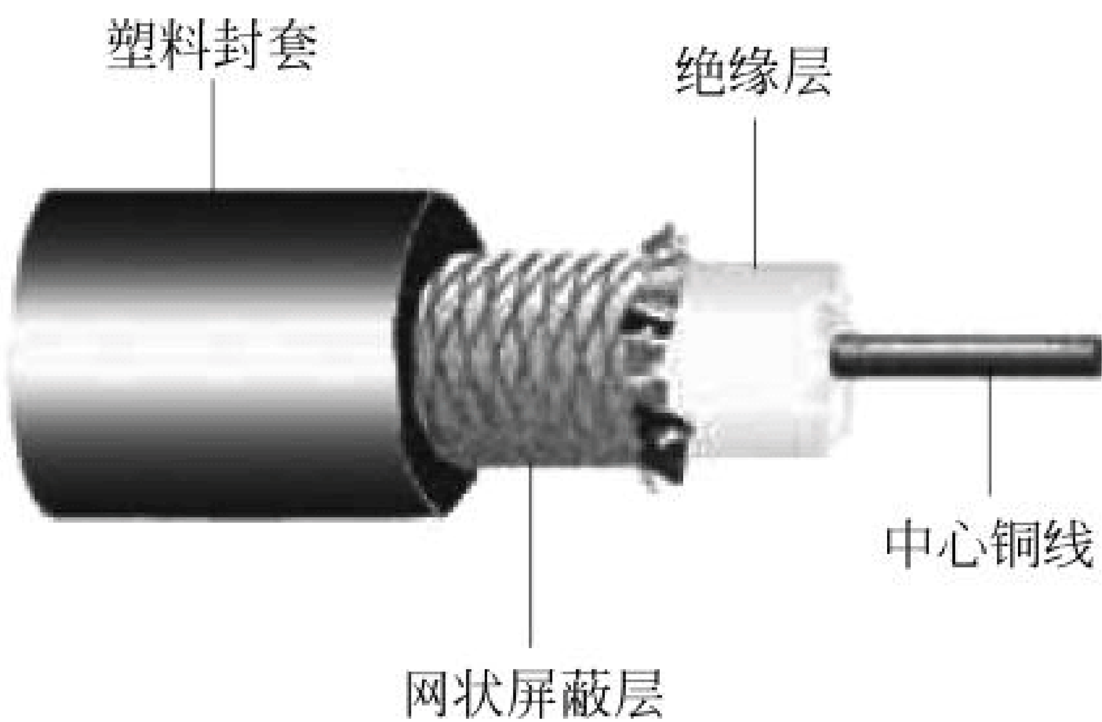


图 2.2　同轴电缆结构示意图

同轴电缆（coaxial cable）是由一根空心的圆柱体及其所包围的单根内导线所组成的，如图 2.2 所示，由里往外依次是铜芯、塑胶绝缘层、细铜丝组成的网状导体及塑料保护膜，铜芯与网状导体同轴，故名同轴电缆或同轴。连接有线电视的信号线即为一种同轴电缆。

同轴电缆的这种结构，决定了其屏蔽性能好、抗干扰能力强，具有更高的带宽和极好的噪声抑制特性，可以更高速度传输更远的距离。同轴电缆的带宽取决于电缆长度，距离越短，带宽越高。

3．光纤

光缆是由一组光纤组成的传输光束的传送介质。与其他通信介质相比，光缆的电磁绝缘性能好、信号衰变小、频带较宽、传输距离大。

1）光纤结构

光缆的核心是光纤，其纤芯是导光性极好、直径很细的柔软圆柱玻璃纤维，光纤由纤芯、包层和涂覆层 3 部分组成，如图 2.3 所示。

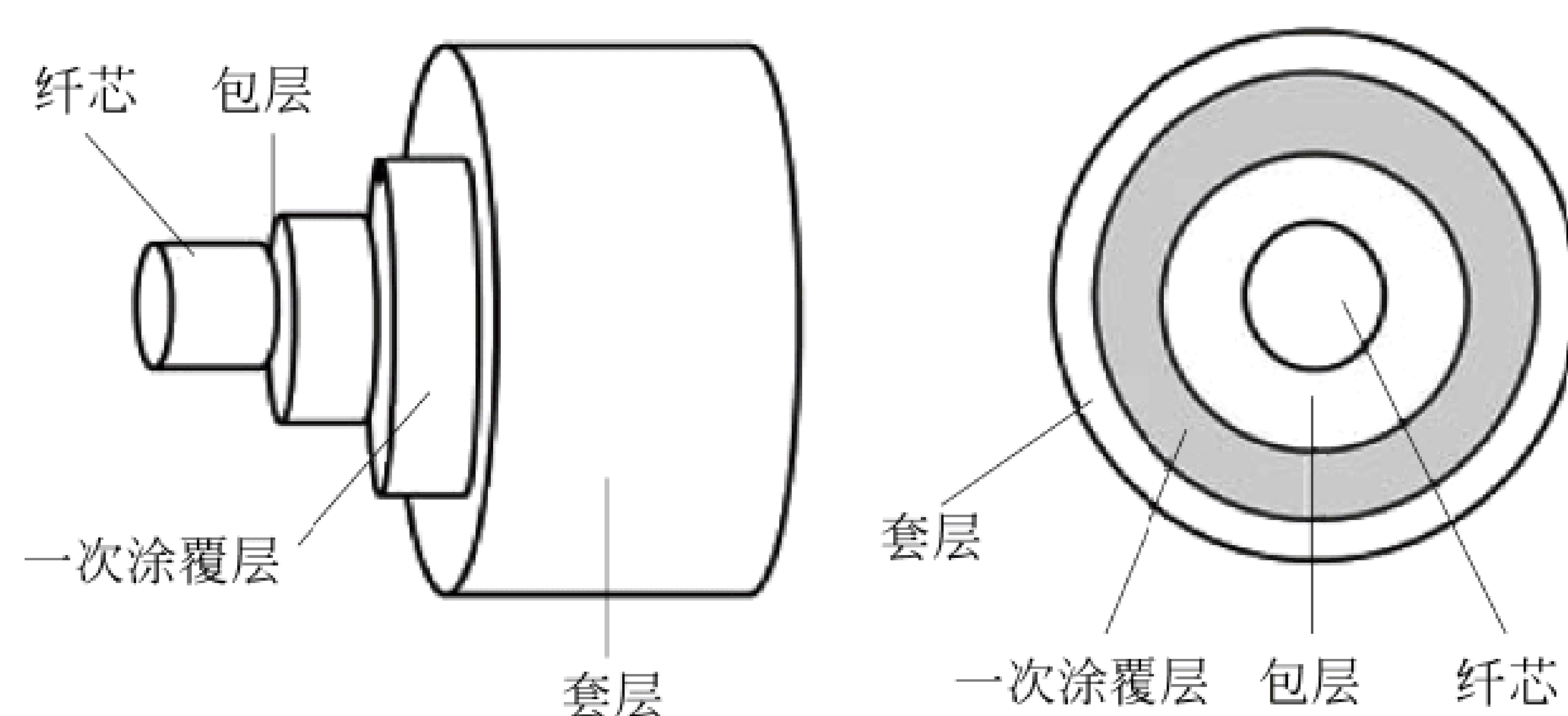


图 2.3　光纤结构

（1）在通信中使用的光纤纤芯和包层一般由石英制成，只是它们分别掺有不同的杂质，以使纤芯的折射率大于包层的折射率，使光波局限于纤芯中传播。纤芯直径一般为 5～75μm，包层直径为 100～150μm。

（2）涂覆层用于保护光纤不受水汽侵蚀和机械擦伤，同时可以增加光纤的机械强度和可弯曲性，延长光纤寿命。涂覆层包括一次涂覆层、缓冲层和二次涂覆层。一次涂覆层是在裸纤表面涂的聚氨基甲酸乙酯或硅酮树脂层，厚度一般为 30～150μm；二次涂覆层也称套层或被服层，多采用聚乙烯塑料或聚丙烯塑料、尼龙等材料。两个涂层之间的缓冲层一般为性能良好的填充油膏，起防水作用。经过二次涂覆的裸纤称为光纤芯线，外径为 1.5mm。

（3）光纤芯线外面的护套，起机械保护作用。

2）光纤分类

（1）根据能同时传输光束的数量，可以将光纤分为单模和多模两种。

单模光纤一般以激光作为光源并且仅允许一束光通过纤芯，即只能传输一路信号，传输距离远，但设备比多模光纤贵。

多模光纤一般以发光二极管作为光源并且允许多路光束通过纤芯，即可以传输多路信号，传输距离较近，设备比单模光纤便宜。

（2）根据折射率的变化，可以将光纤分为阶跃光纤和渐变光纤。阶跃光纤的纤芯和包层的折射率不同，但内部分布都大体均匀，所以在界面上会发生突变。而渐变光纤的纤芯内折射率从中心开始沿半径呈抛物线状递减分布。

图 2.4 为 3 种不同类型光纤的传光原理。

3）光端机

光端机是在光链路的两端使用的设备，主要进行光-电型号的转换。按照使用的位置，分为光发射机和光接收机：光发射机完成电/光转换，并把光信号发射出去用于光纤传输；光接收机主要是把从光纤接收的光信号再还原为电信号，完成光/电转换。

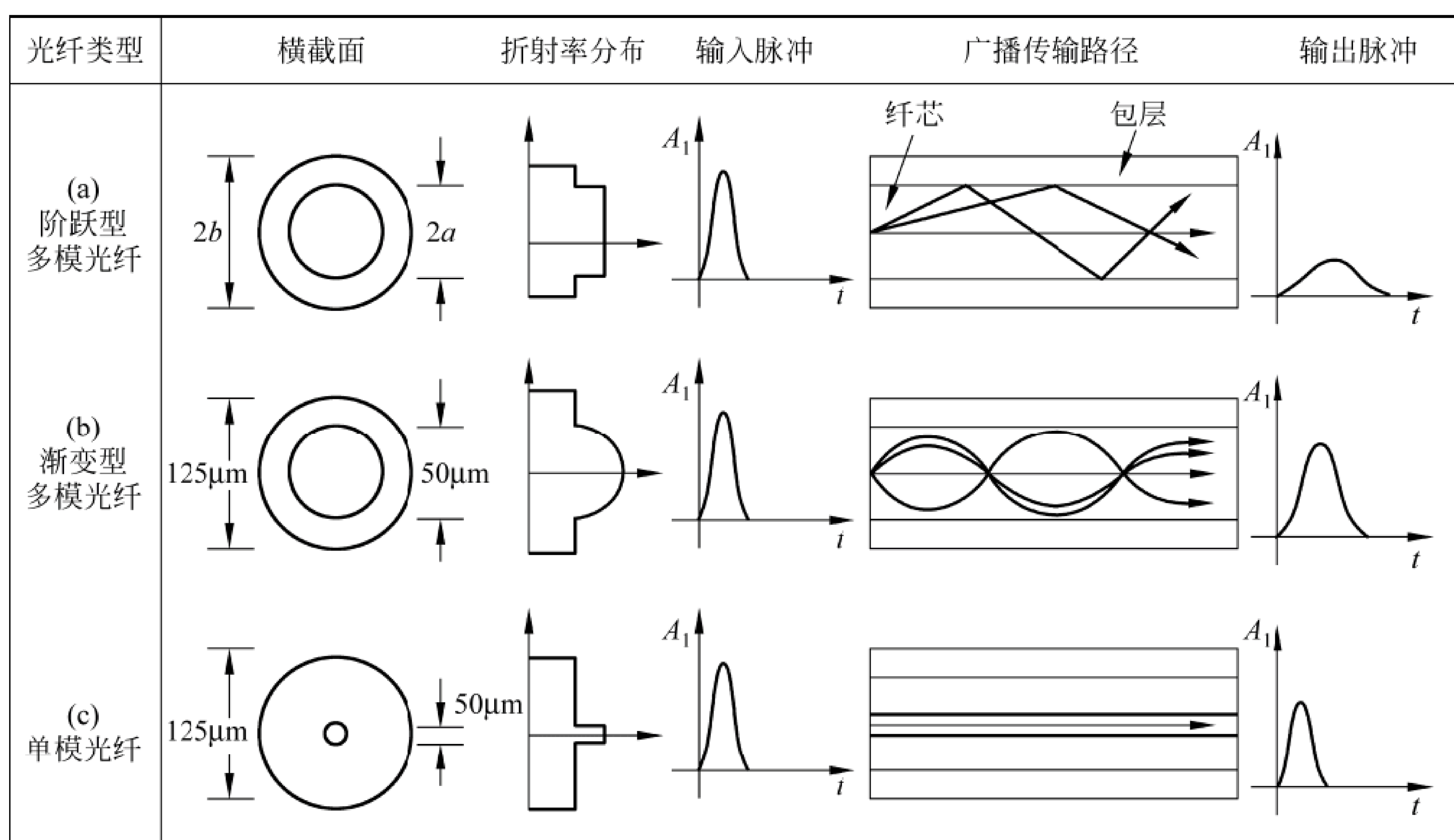


图 2.4　3 种不同类型光纤的传光原理

光端机实际可传输光信号的最大距离是个标称数值，取决于设备和实际环境等多种因素，双纤的光端机一般可传输 1～120km，单纤的一般可传输 1～80km。

按照端口数量，光端机可以分为多口光端机和单口光端机。多口光端机也简称为光端机。单口光端机俗称“光 MODEM”（光猫），适用于本地网中的中继传输设备以及租用线路设备，一般用于用户端。按照端口类型，现有光 MODEM 可以分为如下几种：

（1）单 E1 光端机：将 G.703 的 E1（2048kbps）信号调制到光纤上传输的设备。

（2）单 V.35 光端机：提供一个成帧 N×64kbps 的 V.35（2048kbps）数据接口。

（3）以太网光端机（2Mbps 带宽）：2Mbps 带宽以太网光端机提供一个 2Mbps 带宽的以太网接口（与单 E1 光端机和 E1 转换器配合使用）。

（4）以太网光端机（10Mbps 带宽）：10Mbps 带宽以太网光端机提供一个以太网接口和 4 个 E1 接口。以太网接口带宽 2～10Mbps 可调，当带宽增加时需要占用 E1 接口，每增加 2Mbps 带宽需要占用一个 E1 接口。当以太网带宽为 10M 时，4 个 E1 接口不可用（与 5E1 光端机和 5E1 转换器配合使用）。

4．电力线路载波通信

电力线载波（Power Line Carrier，PLC）也称为电力线通信，是指利用电力线传输数据和媒体信号的通信方式。采用这种技术发送数据时，发送器先将数据调制到一个高频载波上，再经过功率放大后通过耦合电路耦合到电力线上。信号频带峰值电压一般不超过 10V，相对于电力线路的电压幅值是一个很小的值，因此不会对电力线路造成不良影响。在目的端接收信息的适配器再把高频从电流中分离出来并传送到计算机或电话。按照电压等级，电力线路可分为三个等级：高压电力线（在电力载波领域通常指 35kV 及以上电压等级）、中压电力线（指 10kV 电压等级）和低压配电线（380/220V 用户线）。它们都可以作为载波通信介质。

电力线路通信载波具有如下优势：

（1）无须另布网线。利用现有的电力线，无须穿墙打孔来布设网线，作为 PLC 技术的全新应用，能有效避免对建筑物等设施及装修的损坏，节省人力和成本。

（2）有插座的地方就能上网。PLC 技术让分布最为广泛的电力线成为传输多媒体与数据流的载体，实现了有插座的地方就能即插即用地上网，使家庭网络得以拓展和延伸，同时让构建家庭企业局域网络变得轻松简单。

（3）距离稳定传输。利用电力线作为多媒体流与数据流传输的载体，不受障碍物的影响，且承载信号量大、稳定，较传统网线 50～100m 的传输距离有了大幅提升，在同一 220V 的电压下，其传输距离可达 250～300m，若电力回路相对干净，传输距离可高达 450～500m。

（4）节能环保，无辐射。使用电力线进行多媒体与数据流传输，速率高，功耗低。

2.1.2 无线传输介质

无线传输是利用电磁波携带数据信号进行的传输。图 2.5 为一张电磁波频谱图。可以被利用来进行数据传输的部分可以分为两大类：不可见光和可见光。

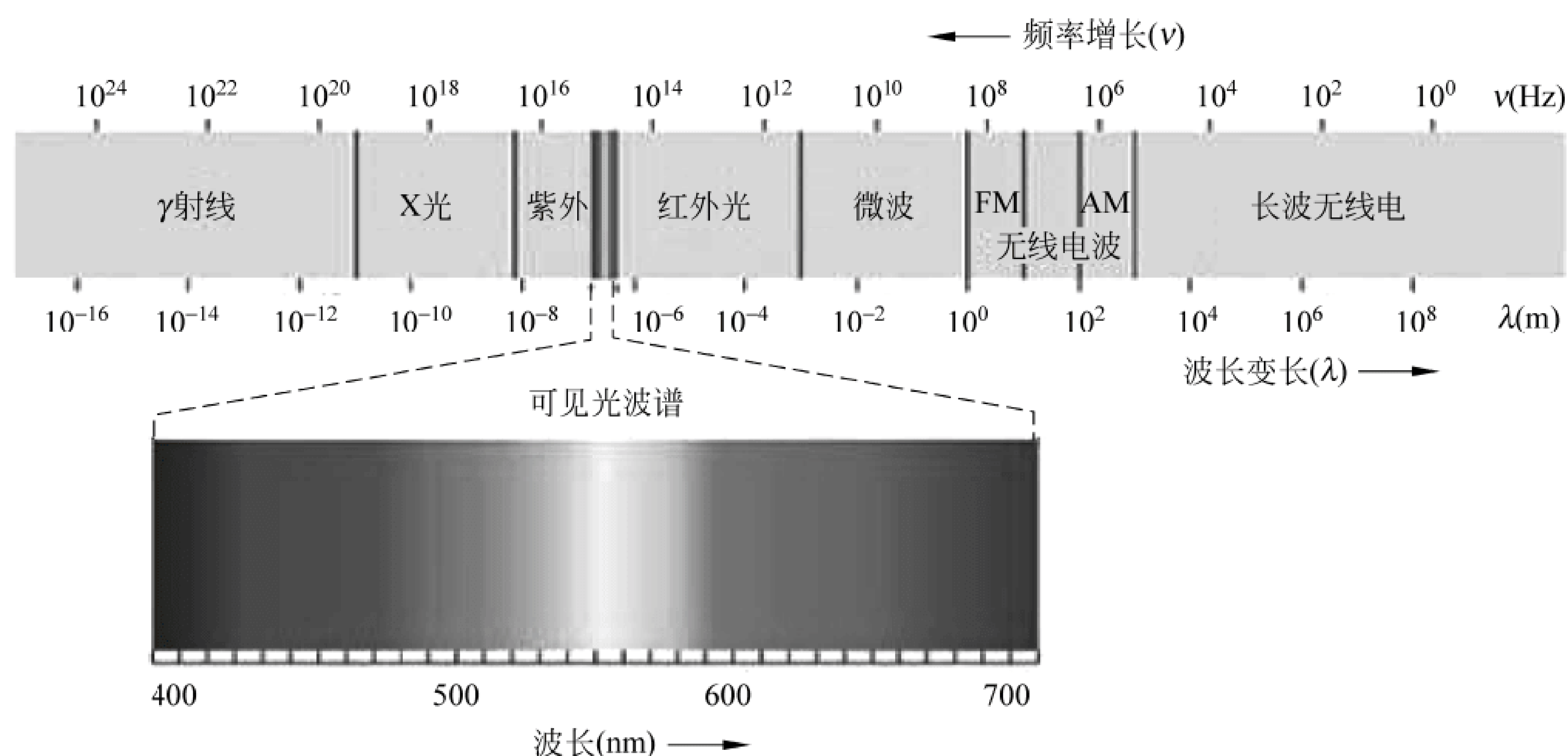


图 2.5 电磁波频谱图

1．不可见光无线传输介质

常用的不可见光数据传输介质包括无线电波、微波、红外光和激光。由于红外线和激光束都具有极强的方向性，并且易受环境（雨、雾和障碍等）影响，只适合短距离（几千米之内）传输，比如各种遥控器大都是用红外线进行信息传输的。另外，激光硬件会发出少量射线，需要特许批准。这里仅讨论无线电波传输，通常分为如下 3 种情况。

1）短距离无线技术

属于在办公室和家庭中使用的短距离无线技术，都能在移动电话、PDA、无线耳机、笔记本、电视、无线打印机、数码相机、投影仪、传感器、等离子屏幕以及其他无线设备间进行无线信息交换。具体有如下几种。

（1）NFC（Near Field Communication，近场通信或称近距离无线通信）——由免接触式

射频识别演变而来，允许电子设备之间进行非接触式点对点数据传输，覆盖范围只有 10cm 左右。

（2）蓝牙（bluetooth）——基于蓝牙技术的电波覆盖半径大约有 15m。

（3）Wi-Fi（wireless fidelity，无线保真）——覆盖半径则可达 100m 左右。

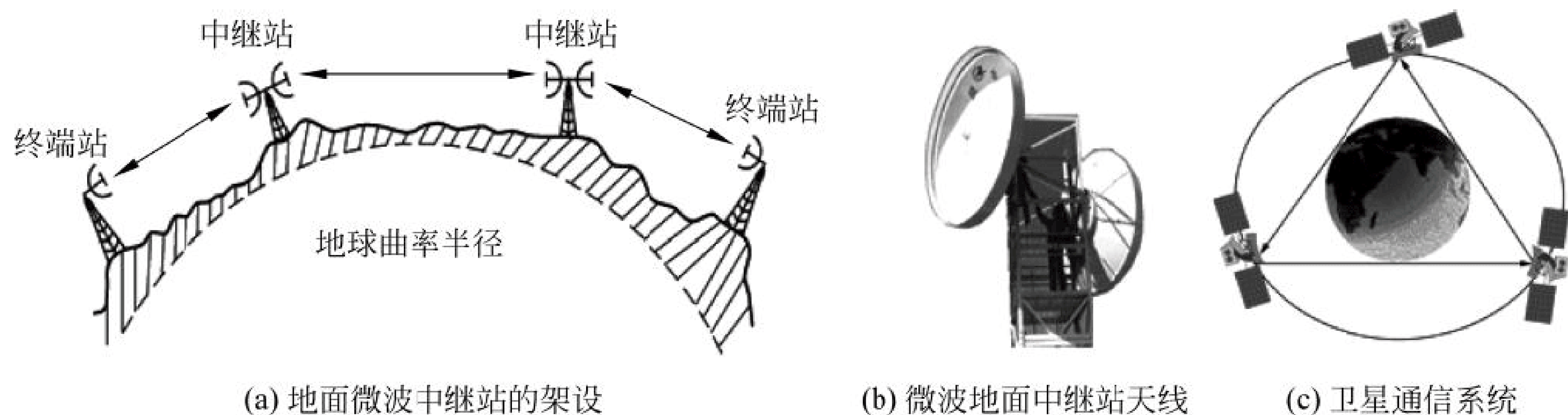
2）中长波无线电波

中长波无线电波主要应用在广播通信中。

3）微波

微波的频带很宽，在数据通信中占有重要的地位。它在空间中是直线传播的，而地球表面呈弧形，因而微波传输距离往往受限，一般最多达到 50km 左右。为了传输更远的距离，必须采取一定的措施。目前，采取的措施主要有地面接力通信和卫星通信两种。

（1）地面接力通信。地面接力通信是指即在地面建立若干微波中继站，进行信号的接力传输。建在地面上的中继站一般站间距离为几万米，为了避免地面上自然或人为的遮挡，地面中继站的天线架设比较高。图 2.6（a）和（b）为微波接力地面中继站的布局及其天线。



(a) 地面微波中继站的架设　(b) 微波地面中继站天线　(c) 卫星通信系统

图 2.6　微波通信

（2）卫星通信。卫星通信是利用与地球相对静止的同步卫星作为中继站的微波接力通信系统，如图 2.6（c）所示。卫星微波通信系统具有通信容量大、传输距离远、覆盖范围广等优点，因此，特别适合于全球通信、电视广播以及恶劣地理环境下使用。例如，美国的全球定位系统 GPS、中国正在组建的“北斗”系统以及欧洲的“伽利略”系统等。从理论上讲，如果在地球赤道上空相对于地球静止的卫星轨道上放置 3 颗间隔各 120° 的卫星，就可以实现全球通信或全球广播。

2．可见光无线传输介质

可见光通信技术（Visible Light Communication，VLC）是利用荧光灯或发光二极管等发出的肉眼看不到的高速明暗闪烁信号来携带数据进行传输。

给普通的 LED 灯泡装上微芯片，可以控制它每秒数百万次闪烁，亮了表示 1，灭了代表 0。由于频率很高，人眼根本觉察不到，光敏传感器却可以接收到这些变化。二进制的数据就被快速编码成灯光信号并进行了有效的传输。灯光下的计算机，通过一套特制的接收装置传输信号。有灯光的地方，就有网络信号。关掉灯，信号全无。

与目前使用的无线局域网（无线 LAN）相比，“可见光通信”系统可利用室内照明设备代替无线 LAN 局域网基站发射信号，其通信速度可达每秒数十兆至数百兆，未来传输速度还可能超过光纤通信。利用专用的、具有收发信号功能的计算机以及移动信息终端，只要

在室内灯光照到的地方，就可以长时间下载和上传高清晰画像或动画等数据。该系统还具有安全性高的特点。用窗帘遮住光线，信息就不会外泄至室外，同时使用多台计算机也不会影响通信速度。由于不使用无线电波通信，对电磁信号敏感的医院等部门可以自由使用该系统。

2.1.3　传输介质的连接

对于不同的传输介质，相应的连接器也不同。图 2.7 为 3 种不同传输介质的连接器。



(a) RJ45连接器(适用于双绞线)　　(b) BNC连接器(适用于同轴电缆)

(c) 常用光纤尾线接头(适用于光缆)

图 2.7　3 种传输介质使用的连接器

2.2　传输控制器

如果说由于微型计算机的普及，导致了若干台微机相互连接，从而产生了局域网的话，那么由于网络的普遍应用，为了在更大范围内实现相互通信和资源共享，网络之间的互联便成为一种信息快速传达的最好方式。网络互连时，必须解决如下问题：在物理上如何把两种网络连接起来；一种网络如何与另一种网络实现互访与通信；如何解决它们之间协议方面的差别；如何处理速率与带宽的差别。解决这些问题，协调转换机制的部件就是中继器、网桥、路由器、接入设备、网关等。

计算机网络中的一些基本的数据通信技术都是在结点上的通信控制设备的控制下实现的。图 2.8 给出了计算机网络中不同结点上的控制设备及其所在的逻辑层次。

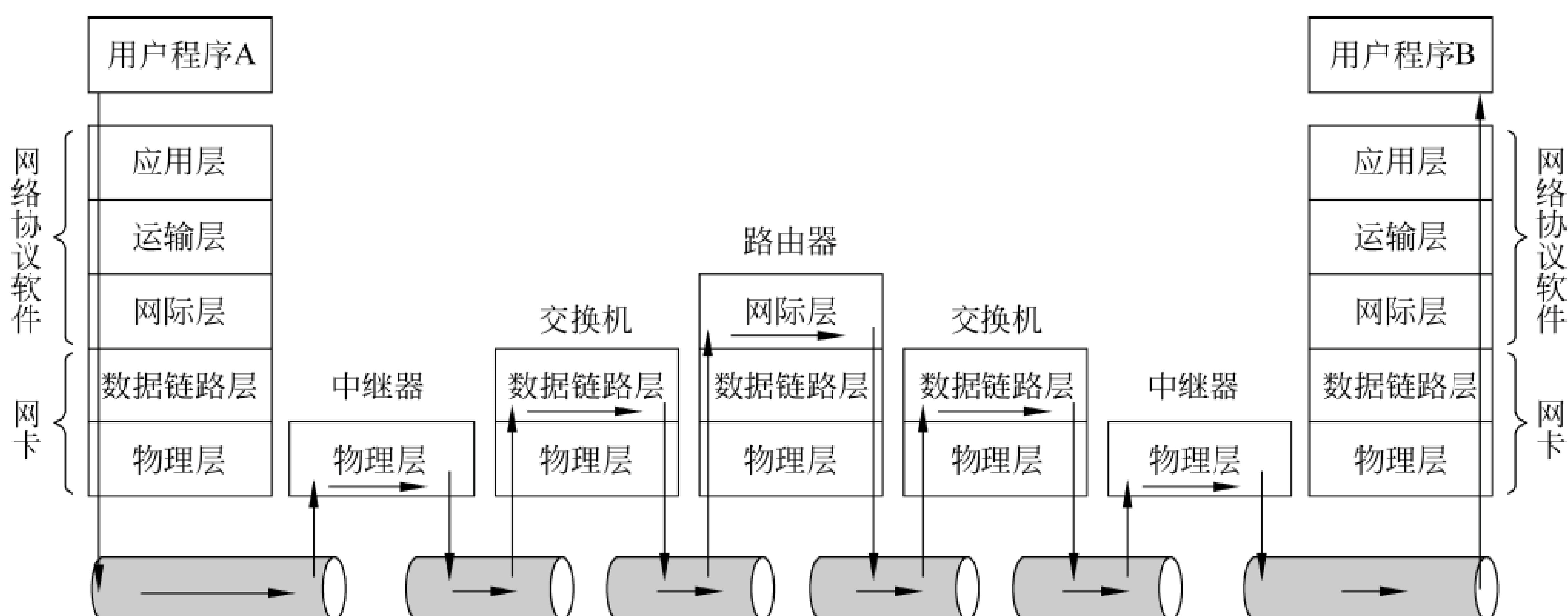


图 2.8　不同层次上的网络通信控制设备

2.2.1　网络适配器

1. 网络适配器及其功能

在网络中是连接计算机与传输介质的接口联网的设备。主要功能是：

（1）用其编号作为计算机的地址。每个网卡都有一个编码。如图 2.9 所示，这个编码由厂商代码和产品代码两部分组成，每一部分为 3 组十六进制码，每组两个，用“-”分隔。厂商代码部分由 IEEE 分配。由于厂商代码和产品代码都是全球唯一的，所以每个网卡的代码也是全球唯一的。IEEE 802 就将此作为设备的 MAC 地址。

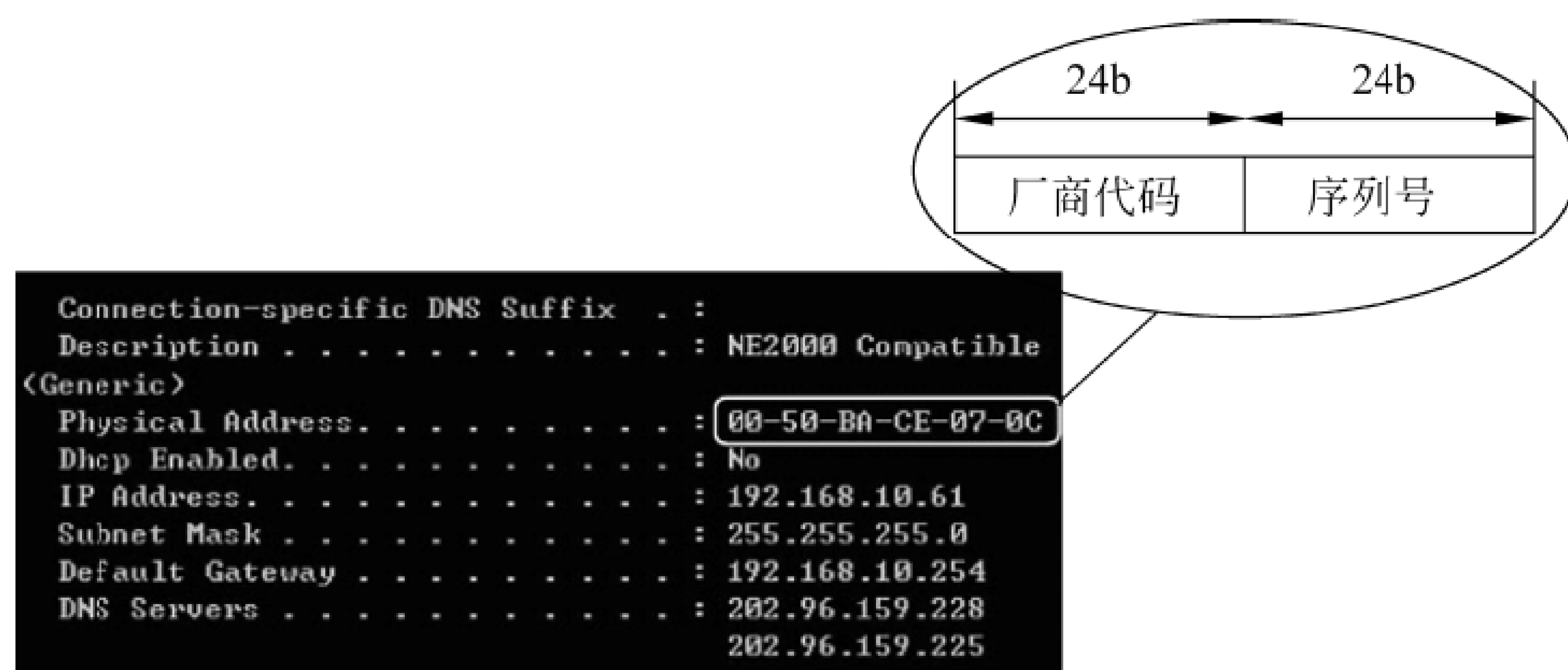


图 2.9　MAC 地址

MAC 地址被用于在网络中标识计算机的物理地址，也称硬件地址或链路地址。这是网卡自身的唯一标识，就仿佛是我们的身份证一样，一般不能随意改变。它与网络无关，无论把这个网卡接入到网络的什么地方，MAC 地址都是不变的。

（2）为计算机进行网络中的数据收发，并检查网络上传来的数据中有无错误，以决定是否接收这个数据。

（3）数据缓冲。

（4）格式转换。

（5）进行链路管理，监听链路上是否有信号冲突。

2. 网卡的基本构造

网卡工作在计算机网络的低两层。所以在一个网络主机的协议体系中，下两层是由网

卡实现的。网卡的结构包括硬件和固件程序（只读存储器中的程序），它们是围绕下两层的实现而设置的。

1）网卡硬件

（1）网卡的控制芯片。网卡的控制芯片是网卡的 CPU，用于控制整个网卡的工作，负责数据的传送和连接时的信号侦测。

（2）晶体振荡器。负责产生网卡所有芯片的运算时钟。通常网卡是使用 20Hz 或 25Hz 的晶体振荡器。千兆网卡使用 62.5MHz 或者 125MHz 晶振。

（3）调控元件。用来发送和接收中断请求 IRQ，指挥数据的正常流动。

（4）网络接头，用于连接网络。在用双绞线作为传输媒介时，基本采用 RJ-45 接头；用细同轴电缆作为传输媒介时，采用 BNC 接头。

（5）信号指示灯。通常有两个信号：TX 代表正在送出数据，RX 代表正在接收数据。通过不同的灯光变换来表示网络是否导通。

2）固件程序

固件程序实现逻辑链路控制和媒体访问控制的功能，还记录 MAC 地址。

3）其他

（1）缓存和收发器（transceiver）。

（2）BOOT ROM，即启动芯片等。

注意：光安装了网卡，还不能使用网卡，还必须安装相应的网卡驱动程序（device driver）。网卡驱动程序是操作系统中的一个模块，它包含了网卡的有关信息。操作系统根据这些信息才能给网卡配置所需要的资源。网卡驱动程序通常由网卡厂商开发，可以在网卡厂商的官方网站下载，有些操作系统已经包含了许多标准网卡驱动程序。

2.2.2 中继器

信号在介质中传输时，随着传输距离的增加，幅度将会逐渐衰减，波形将会产生失真。中继器（repeater）用于同类网络介质之间的互连，起到信号再生、放大作用。再生就是通过对失真的但仍可以辨认的波形的分析，重新生成原来的波形；放大就是将信号衰减了的幅度加以恢复。通过再生和放大能够使网络传输的距离范围得以扩大。图 2.10 简单地说明了中继器的基本工作原理。这是一种一通一的中继。中继还有一通多的中继，称为集线器（Hub）。

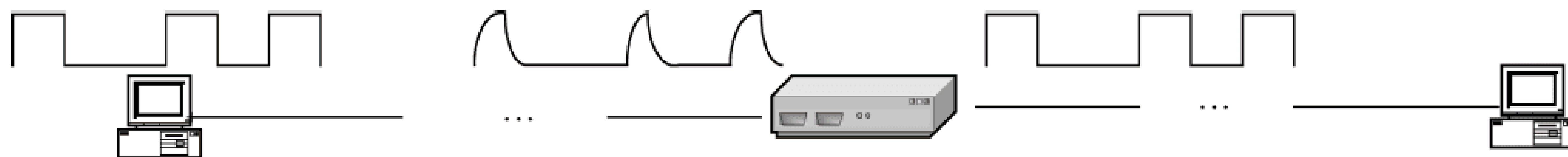


图 2.10　中继器的工作原理

Hub 按配置形式可分为独立型集线器、模块化集线器和堆叠式集线器三种；按其端口分，Hub 有 8 端口、16 端口、24 端口等几类；按其传输速率分，有 10Mbps、100Mbps 和 10/100Mbps 集线器等几种。不同的通信介质有不同的中继器，例如微波中继器、卫星中继器、用于同轴电缆的双口中继器（连接两段同轴电缆）和多口中继器（用于扩展 3 个或 3 个以上网段），以及用于多条双绞线连接的集线器等。

使用 Hub 连接具有如下特点：

（1）目前 Hub 主要用于在星形结构的中央结点上连接多条无屏蔽双绞线，设备的接入或退出比较灵活、方便，也便于维护，当某一设备或某一网段发生故障时，可以简单地卸掉，不扩大故障范围，不影响其他结点的正常工作，便于维护。

（2）Hub 属于物理层的连接设备，工作都与地址无关，因此 Hub 所连接的各条链路之间的信号具有共享性，只能以广播传送方式工作。即一个端口的输入信号，经整形、放大后可以转发到其他所有连接的链路或网段上。

（3）Hub 的所有端口共享上行带宽方式。例如，当上行带宽为 10Mbps 的集线器时，若连接了两个设备，则每个设备只有 5Mbps 的带宽；若连接了 10 个设备，则每个设备就只有 1Mbps 的带宽了。这会增加网络塞车风险，降低了网络执行效率。

（4）共享式网络是一种无管理疏导的无序工作状态，每个客户端都会尽可能地抢占通信通道，因此常常形成网络堵塞的局面，当数据和用户数量超出一定的限量时，就会造成网络性能的严重衰退。连接的端口数目越多，就越容易造成冲突。依据经验，一个 10Mbps 集线器所管理的计算机数不宜超过 15 个，100Mbps 的不宜超过 25 个。

2.2.3　交换机

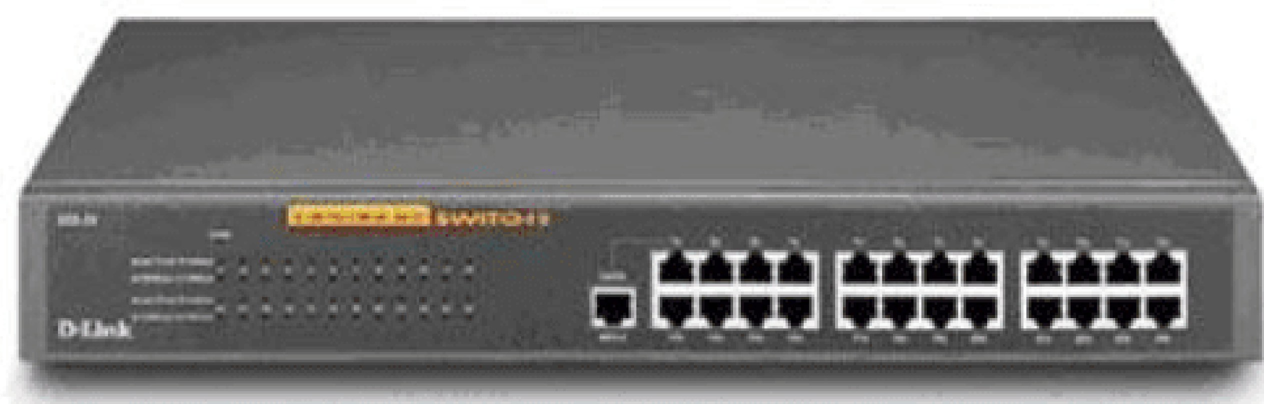


图 2.11　交换机

现代通信网络按照有无交换功能可以分为两大类：交换网与传输网。传输网没有交换功能，仅仅用于数据传输。例如，DDN（Digital Data Network，数字数据网）就没有交换功能，一般用于向用户提供专线传输服务。在交换网中，数据交换是由交换机实现的，如图 2.11 所示为一个交换机的示例，可以看到，交换机有许多端口，交换就在这些端口之间进行。

广义的交换机是完成数据交换的设备。有工作在 OSI 第 2 层的交换机，也有工作在 OSI 第 3 层的交换机。这里介绍的交换机是工作在第 2 层，即数据链路层的交换设备，所交换的对象是帧，也就是转发帧。

1．交换机的功能

交换机是交换网的交通枢纽，其作用是将接收到的数据有选择地转发到其他端口，实现交换网中的数据流控制。下面进一步说明。

（1）“有目的地”地转发数据。当有比特流送到交换机端口时，交换机就先接收并将之保存在缓冲区内，由数据链路层对帧头进行分析，并按照帧头中的目的地址将该帧装发到可以到达目的地址的端口。

（2）分隔冲突域。所有共享同一传输介质的站点属于同一冲突域。对于交换机来说，同一端口连接的站点属于同一冲突域，不同端口连接的站点属于不同的冲突域。与集线器相比，交换机可以分隔冲突域，减少冲突。在每个端口只有一个站点的极限情况下，就可以完全避免冲突。

（3）流量控制。给不同的端口分配带宽，延缓数据的传输能力。例如，可以给某些端口分配带宽为 100Mbps，同时给另一些端口分配带宽为 10Mbps，而不是像集线器那样共享平均分配带宽。这使交换机能够提供更佳的通信性能。

（4）可以提供全双工通信，与半双工通信相比，可以把带宽提高一倍。

（5）其他。

- 物理编址：定义数据帧的物理地址；
- 网络拓扑结构设定：定义设备物理连接所形成的网络拓扑结构；
- 差错验证：错误发生时发出报警；
- 数据帧整序。

2．交换机的工作原理

交换机进行数据转发的依据是主机的物理地址。如图 2.12 所示，交换机有两个关键部件：地址表和交换机构。地址表中记录的是主机的物理地址（即其网卡编号——MAC 地址）及其与交换机端口的对应关系。当交换机的输入端口接收到一个帧时，先存储起来，然后分析该分组的目的地址，再按照这个地址从地址表中找到对应的端口，将这个帧送到这个端口的发送队列中进行发送。地址表是交换机上电后自动建立的。

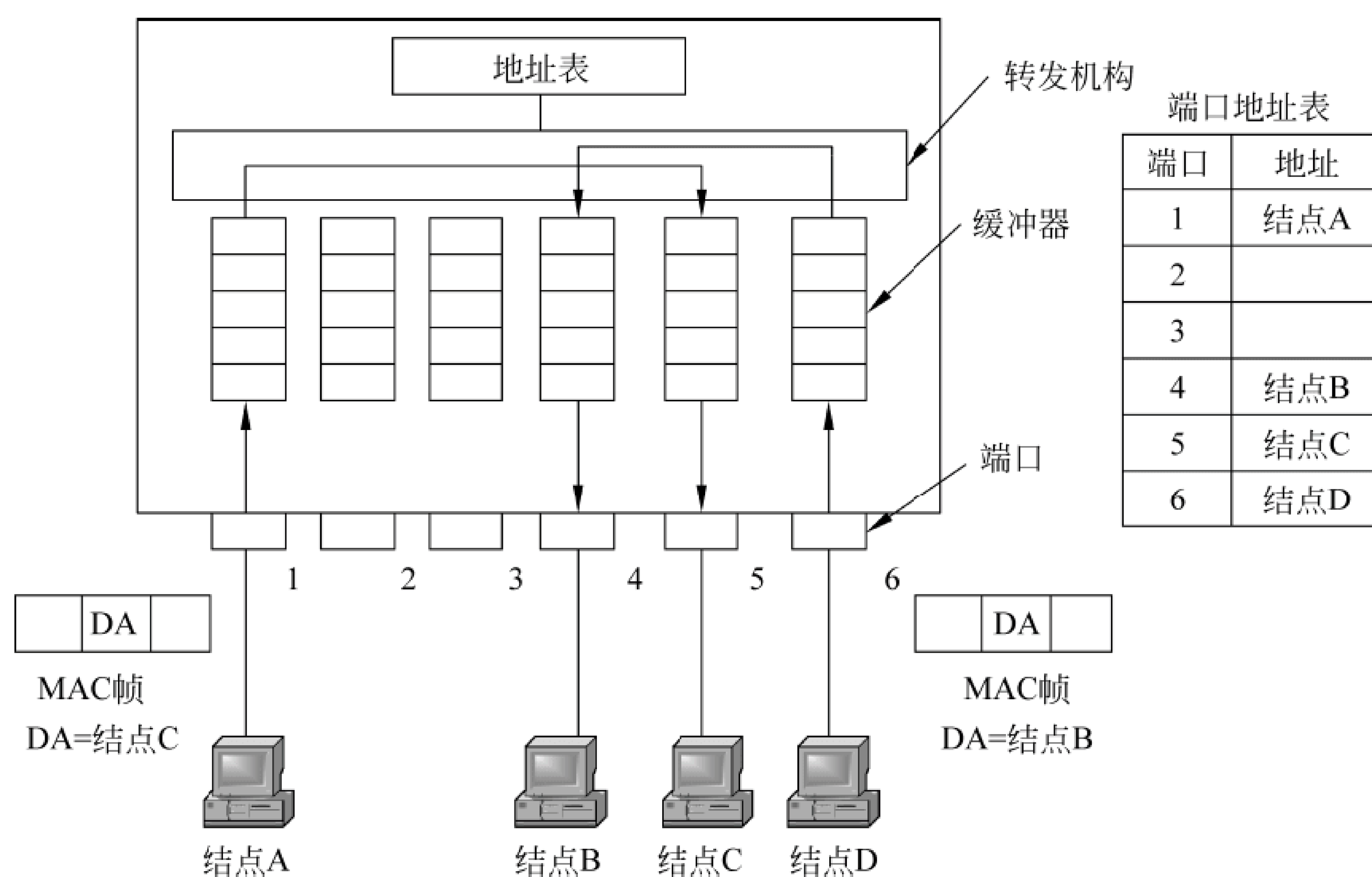


图 2.12　交换机原理

3．交换机的分类

1）按照带宽分类

- 10M 交换机：只支持 10Mbps 端口。
- 100M 交换机：只支持 100Mbps 端口。
- 10M+100M 交换机：一部分端口支持 10Mbps，另一部分端口支持 100Mbps。
- 100M+1000M 交换机：一部分端口支持 100Mbps，另一部分端口支持 1000Mbps。
- 10M+100M+1000M 交换机：一部分端口支持 10Mbps，另一部分端口支持 100Mbps，

还有一部分端口支持 1000Mbps。

现在，许多交换机做成了 10Mbps、100Mbps 和 1000Mbps 的自适应端口，用户使用起来更方便。

2）按应用场合分类

- 工作组级交换机：用于小型局域网的组建，如办公室局域网、小型机房、家庭局域网等。这类交换机的端口一般为 10/100Mbps 自适应端口。
- 部门级交换机：常用来作为扩充设备，当工作组级交换机不能满足要求时可考虑使用部门级交换机。这类交换机只有较少的端口，但支持更多的 MAC 地址。端口的传输率一般为 100Mbps。
- 企业级交换机：用于大型网络，且一般作为网络的骨干交换机。企业级交换机一般具有高速交换能力，并且能实现一些特殊功能。

4. 交换机与集线器的区别

（1）从 OSI 体系结构来看，集线器属于 OSI 的第 1 层物理层设备，而交换机属于 OSI 的下两层的设备。这就意味着集线器只是对数据的传输起到同步、放大和整形的作用，对数据传输中的短帧、碎片等无法有效处理，不能保证数据传输的完整性和正确性；而交换机不但可以对数据的传输做到同步、放大和整形，而且可以过滤短帧、碎片等。

（2）从工作方式来看，集线器是一种广播模式，也就是说，集线器的某个端口工作的时候其他所有端口都能收听到信息，容易产生广播风暴。当网络较大的时候，网络性能会受到很大的影响，那么用什么方法避免这种现象的发生呢？交换机就能够起到这种作用。当交换机工作的时候只有发出请求的端口和目的端口之间相互响应而不影响其他端口，那么交换机就能够隔离冲突域和有效地抑制广播风暴的产生。

（3）从带宽来看，集线器不管有多少个端口，所有端口都共享一条带宽，在同一时刻只能有两个端口传送数据，其他端口只能等待；集线器只能工作在半双工模式下。而对于交换机而言，每个端口都有一条独占的分配带宽，当两个端口工作时并不影响其他端口的工作；交换机既可以工作在半双工模式下，也可以工作在全双工模式下。

2.2.4 光交换

光交换（photonic switching）是指不经过任何光/电转换，将输入端光信号直接交换到任意的光输出端。光交换是全光网络（All Optical Network，AON）的关键技术之一。

所谓全光网络，是指信号只是在进出网络时才进行电/光和光/电的变换，而在网络中传输和交换的过程中始终以光的形式存在。全光网可以克服电子交换在容量上的瓶颈限制；可以大量节省建网成本；可以大大提高网络的灵活性和可靠性，是未来宽带通信网的发展方向。

1. 光交换系统的构成

如图 2.13 所示，光交换系统主要由输入接口、光交换矩阵、输出接口和控制单元 4 部分组成。

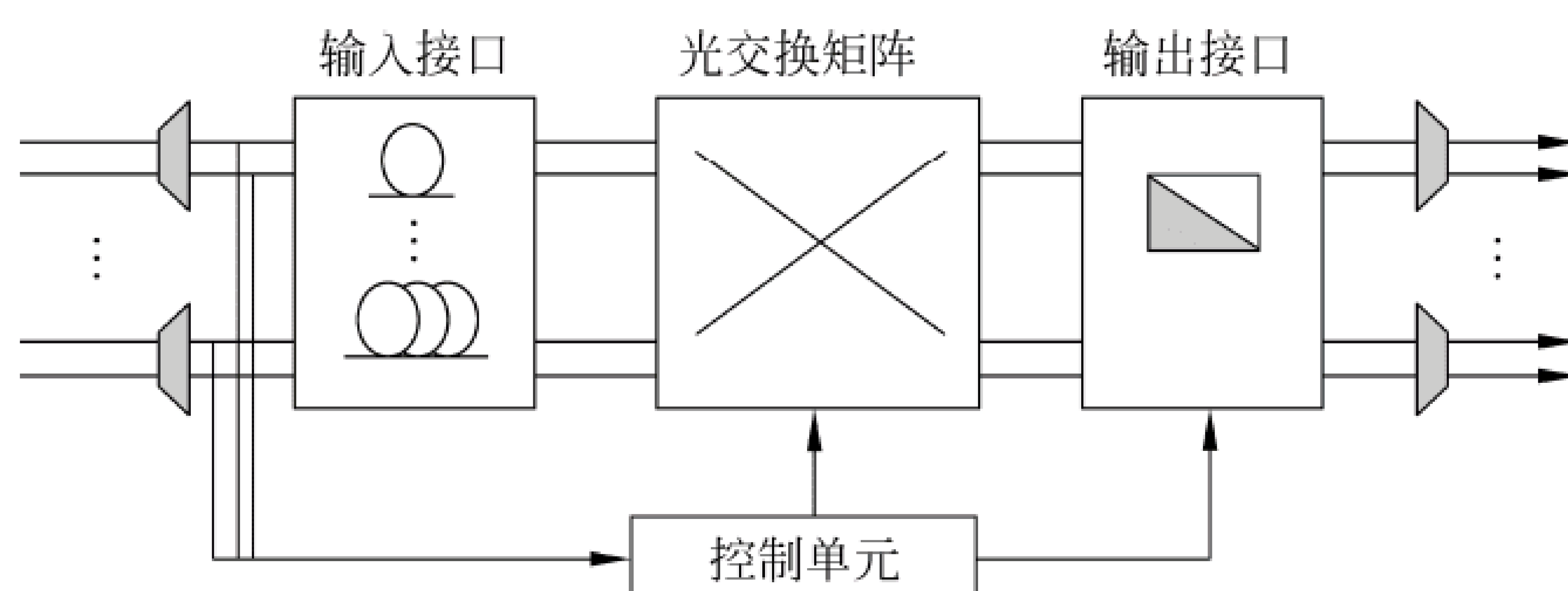


图 2.13　光交换系统的组成

由于目前光逻辑器件的功能还较简单，不能完成控制部分复杂的逻辑处理功能，因此现有的光交换控制单元还要由电信号辅助完成，即所谓的电控光交换。在控制单元的输入端进行光电转换，而在输出端需完成电光转换。随着光器件技术的发展，光交换技术的最终发展趋势将是光控光交换，即全光交换。实现全光交换的关键部件有如下几种。

（1）光逻辑器件：该类器件由光信号控制它的状态，用来完成光信号的各类布尔逻辑运算。

（2）光缓存器件。光缓存器件对光信号进行缓存，是实现光分组交换的关键技术。

（3）波长变换器。全光波长转换器实现光信号传输波长的变换，是在波分复用光网络中实现全光交换的关键部件。

2. 光路交换与光分组交换

与传统的基于电的交换类似，光交换技术可分成光路交换和光分组交换两种主要类型。

1）光路交换

光路交换（Optical Circuit Switch，OCS）技术类似于现存的电路交换技术，需要一个建立与拆除的过程。这个过程采用光交叉连接器（Optical Cross Connection，OXC）、光分插复用设备（Optical Add/Drop Multiplexer，OADM）等光器件实现。

OCS 的协议机制相对简单，技术成熟，易于实现，但其建立和拆除过程要花费一定的时间，并且该时间与它连接的保持时间无关。当连接保持时间比较短时，将导致信道的利用率变差。因此不适合于持续增长且变化频繁的 TCP/IP 流量，如网页浏览、FTP 文件传输、电子邮件等。进一步说，未来的光网络要求支持多粒度的业务，其中小粒度的业务是运营商的主要业务，业务的多样性使得用户对带宽有不同的需求，而 OCS 在光子层面的最小交换单元是整条波长通道上数 Gbps 的流量，很难按照用户的需求灵活地进行带宽的动态分配和资源的统计复用，所以光分组交换应运而生。

2）光分组交换

光分组交换（Optical Packet Switch，OPS）。它以光分组作为最小的交换颗粒，数据包的格式为固定长度的光分组头、净荷和保护时间三部分。在交换系统的输入接口完成光分组读取和同步功能，同时用光纤分束器将一小部分光功率分出送入控制单元，用于完成如光分组头识别、恢复和净荷定位等功能。光交换矩阵为经过同步的光分组选择路由，并解决输出端口竞争问题。最后输出接口通过输出同步和再生模块，降低光分组的相位抖动，同时完成光分组头的重写和光分组再生。

光分组交换在带宽利用率、延时和适应性等方面比较好，从长远的角度来考虑，是一

种很有前途的技术。但是它的实现比较复杂，其中的关键技术，如光逻辑处理技术、光随机存储器（Optical RAM，ORAM）技术都还在研究之中。

2.2.5 路由器

如图 2.14 所示，路由器（router）是位于几个网络边界上的设备，其主要作用是为到达网络边界的数据分组选择一条继续转发的路径——进行路由选择（routing）。作为不同网络之间互相连接的枢纽，路由器系统构成了基于 TCP/IP 的 Internet 的主体脉络，也就是说，路由器构成了 Internet 的骨架。路由器的处理速度是网络通信的主要瓶颈之一，它的可靠性则直接影响着网络互连的质量。因此，在园区网、地区网乃至整个 Internet 研究领域中，路由器技术始终处于核心地位，其发展历程和方向成为整个 Internet 研究的一个缩影。

1. 路由器的基本功能

路由器（router）是工作在 OSI 模型网络层的设备，是按照 IP 地址进行数据转发的设备。这个 IP 地址是根据路由算法计算得到的，可能是一台主机的 IP 地址，也可能是下一台路由器的 IP 地址。

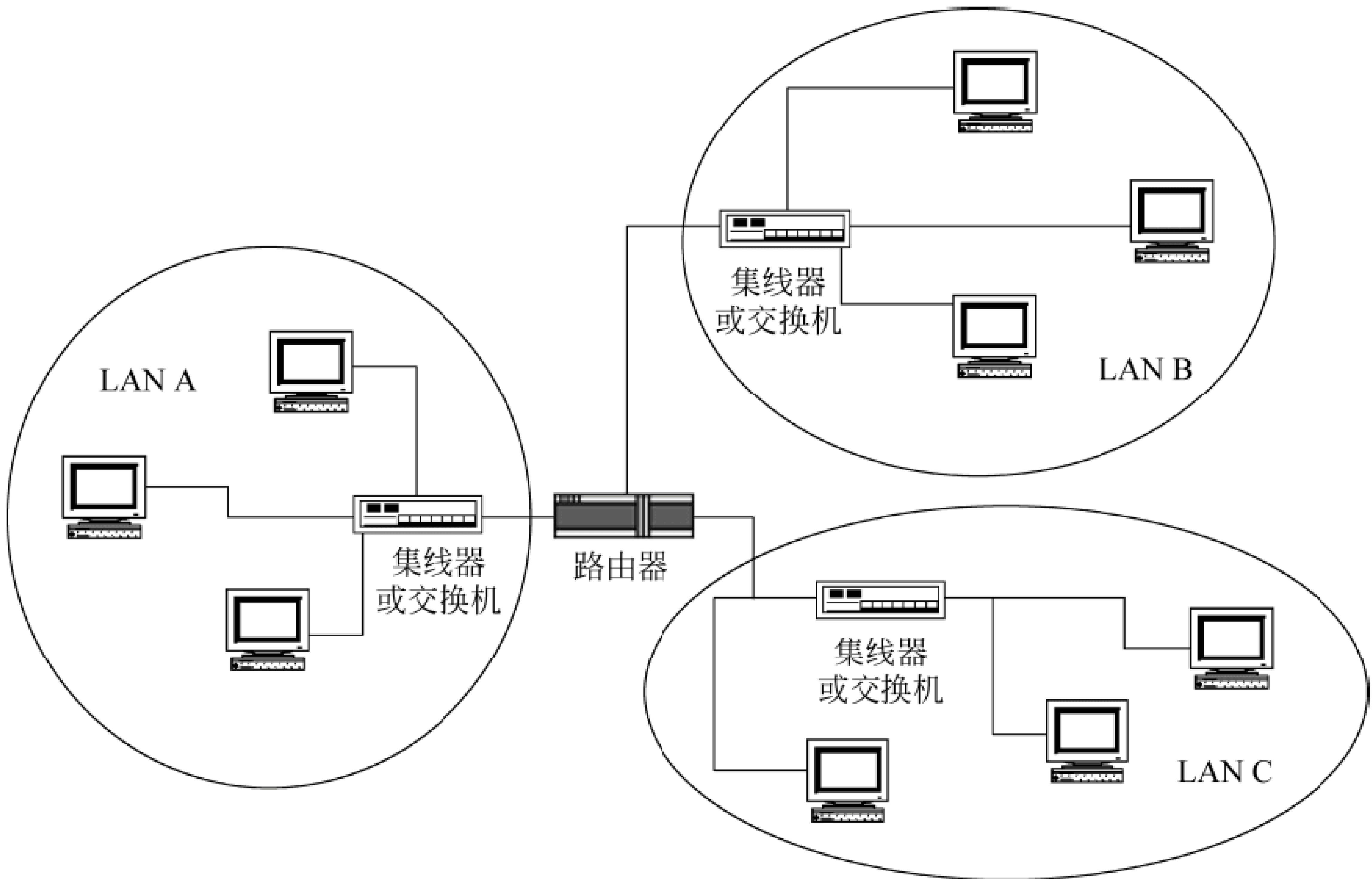


图 2.14　路由器与交换机的位置区别

简单地说，路由器的主要工作有以下两个。

（1）路径判断，使用一定的路由算法选择合适路径。

（2）转发。

2. 路由器的构成

一个路由器是一种具有多输入端口和多输出端口的计算机系统。如图 2.15 所示，路由器的接口主要有串口、以太口、CONSOLE 口等。串口连接广域网，以太口连接局域网，而 CONSOLE 口用于连接计算机或终端，配置路由器（路由器在使用前必须进行相应的配置，

才能正常工作。通常可以将一台计算机连接到路由器的 CONSOLE 口上，通过计算机对路由器进行相应的配置）。

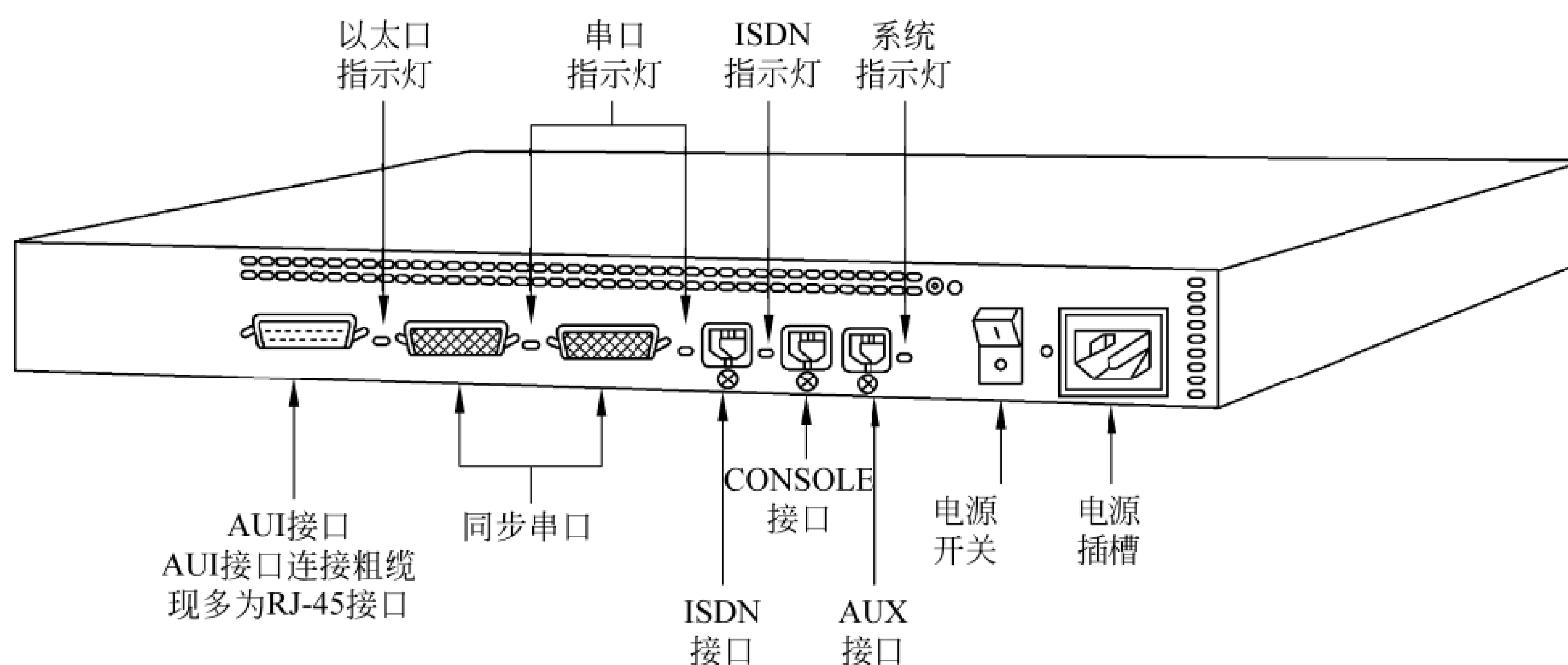


图 2.15　路由器的端口

路由器由路由选择和分组转发两部分组成。

1）路由选择部分

路由选择部分主要由路由表和路由处理器所组成。

（1）路由表。

路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径，并将该数据帧有效地传送到目的站点。为此，每个路由器中都要维护一个路由表（routing table），供路由选择时使用。

路由表中保存着子网的标志信息、网上路由器的个数、下一个路由器的名字等内容。以目的地址作为关键字，就可以从路由表中查出下一站路由器的地址以及它所在的接口。因此，路由表就成为路由器的中枢，它决定了每个数据包的转发方向。

路由表可以是由系统管理员固定设置好的，也可以由系统动态修改，可以由路由器自动调整，也可以由主机控制。

（2）路由处理器。

无论在中低端路由器还是在高端路由器中，CPU 都是路由器的心脏，其主要任务是依据所选路由协议来构建并维护路由表。通常在中低端路由器中，CPU 的能力直接影响路由器的吞吐量（路由表查找时间）和路由计算能力（影响网络路由收敛时间）。在高端路由器中，通常包转发和查表由 ASIC 芯片完成，CPU 只实现路由协议、计算路由以及分发路由表。由于技术的发展，路由器中许多工作都可以由硬件（专用芯片）实现。CPU 性能并不完全反映路由器性能。路由器性能由路由器吞吐量、时延、路由计算能力等指标体现。

它通过计算和交换路由信息、路由表查找以及转发数据包实现路由协议，并运行对路由器进行配置和管理的软件。

除了 CPU，还需要一组供 CPU 使用的存储器。

2）分组转发部分

分组转发部分主要由交换结构、一组输入端口和一组输出端口组成，通常有三类端口：

（1）局域网端口，主要有 AUI 端口、BNC 和 RJ-45 口。

（2）广域网端口，主要有 AUI 和高速同步串口等。

（3）路由器配置端口，如 Console（本地配置端口）和 AUX（远程配置端口）。

3. 路由器的主要类型

（1）按照路由器在自治域（被运营商划分出的网络小群）中的位置可分为以下两种：

- 内部路由器——在自治域内部转发数据包；
- 边界路由器——在不同自治域之间转发数据包。

（2）按所支持的协议可分为以下两种：

- 单协议路由器——仅支持单一协议；
- 多协议路由器——可以支持多种协议传送。

（3）按所连接的范围，路由器分为以下 3 种：

- 接入路由器——连接家庭或 ISP 内的小型企业客户，接入路由器不仅要提供 SLIP 或 PPP 连接，还支持诸如 PPTP 和 IPSec 等虚拟专用网络协议；
- 企业或校园级路由器——主要目标是以尽量便宜的方法实现尽可能多的端点互连，并且进一步要求支持不同的服务质量；
- 骨干级路由器实现企业级网络的互连，对它的要求是速度和可靠性，而代价则处于次要地位。

（4）路由器还可以记录经过的数据包，将之保存到日志中，供网络管理（认证、审计、受费等）使用；还可以在网络之间建立一个“阻塞点”，在可信任网络和不可信任网络之间形成隔离，进行数据的进出检查，形成一个“防火墙”。

2.3 网 络 软 件

网络软件主要包括网络操作系统、网络通信协议以及网络管理和服务用软件。

2.3.1 网络操作系统

1. 网络操作系统及其功能

操作系统（OS）是计算机系统中负责管理计算机资源，为应用程序提供运行环境以及为用户提供操作环境的系统软件。网络操作系统（NOS）则是负责管理网络环境下的计算机资源，为应用程序提供网络运行环境以及为用户提供网络操作环境、支持网络通信、提供网络服务的程序集合。具体地说，网络操作系统除了应具有通常操作系统应具有的处理机管理、存储器管理、设备管理和文件管理外，还应具有以下 4 大功能：

（1）提供高效、可靠的网络通信能力。

（2）提供多种网络服务功能，如远程作业录入并进行处理的服务功能、文件传输服务功能、电子邮件服务功能、远程打印服务功能等。

（3）包括网卡在内的各种设备驱动程序。

（4）由于客户-服务器方式已经在计算机网络中得到广泛应用，因此网络操作系统因客户端与服务器端的环境和需求不同，网络操作系统的功能也有不同。特别是服务器端的网络操作系统，要具有更多的网络支持功能。

2．LAN 中的网络操作系统

由于网络计算的出现和发展，现代操作系统的主要特征之一就是具有上网功能。因此，目前所有操作系统都毫无例外地具有了网络操作系统的特征，人们也不再特指某个操作系统为网络操作系统。这些操作系统主要有如下几种，每一类操作系统又分为客户端操作系统和服务器端操作系统。

1）Windows 族系统

目前 Windows 网络操作系统几乎成为中小型企业局域网的标准操作系统，一则是它继承了 Windows 家族统一的界面，使用户学习、使用起来更加容易；再则它的功能也的确比较强大，基本上能满足所有中小型企业的各项网络需求。

2）UNIX 系统

目前常用的 UNIX 系统版本主要有 UNIX SUR4.0、HP-UX 11.0、Sun 的 Solaris 8.0 等。支持网络文件系统服务，提供数据等应用，功能强大，由 AT&T 和 SCO 公司推出。这种网络操作系统稳定和安全性能非常好，但由于它多数是以命令方式进行操作的，不容易掌握，特别是初级用户。UNIX 一般用于大型的网站或大型的企、事业单位局域网中。

3）Linux 系统

这是一种新型的网络操作系统，它的最大的特点就是源代码开放，可以免费得到许多应用程序。目前也有中文版本的 Linux，如 REDHAT（红帽子）、红旗 Linux 等。在国内得到了用户的充分肯定，主要体现在它的安全性和稳定性方面，它与 UNIX 有许多类似之处。但目前这类操作系统目前使仍主要应用于中高档服务器中。

2.3.2　网络协议软件

1. 通信软件

通信软件是用来监督和控制通信工作的软件。它除了作为计算机网络的基础软件外，还可以为计算机与自带终端或附属计算机之间的通信提供服务。通信软件通常由线路缓冲区管理程序、线路控制程序以及报文管理程序组成。线路控制程序用于同步控制、流量控制以及调制/解调；报文管理程序通常由接收、发送、收发记录、差错控制、开始和终了 6 个部分组成。这些程序中有些已经被固化。

2. 高层协议软件

高层协议软件按协议层次模型（如 ISO 建议的开放系统互连基本参考模型）组织而成。各层协议的主要任务是完成相应层协议所规定的功能以及与上、下层的接口功能。在 TCP/IP 体系中，高层协议就是应用层协议，主要用于提供资源服务。

2.3.3 网络管理软件

1. 网络管理的功能

网络管理具有如下 5 大功能：

（1）故障管理（fault management）。当网络发生故障时实现如下功能：

- 尽可能快地找出故障发生的确切位置。
- 将网络其他部分与故障部分隔离，以确保网络其他部分能不受干扰继续运行。
- 重新配置或重组网络，尽可能降低由于隔离故障后给网络带来的影响。
- 修复或替换故障部分，将网络恢复为初始状态。

（2）计费管理（accounting management）。实现如下功能：

- 统计哪些用户、使用何信道、传输多少数据，访问什么资源等信息。
- 记录、统计网络资源的使用情况，以控制和检测网络操作的费用和代价。

（3）配置管理（configuration management）。负责初始化网络并配置网络，包括：

- 识别被管理网络的拓扑结构。
- 标识网络中的各种现象。
- 自动修复指定设备的配置。
- 动态维护网络配置数据库等内容。

（4）性能管理（performance management）：评估系统资源的运行情况及通信效率情况，以便在最少的网络资源和具有最小延迟的前提下，确保网络能提供可靠、连续的通信能力，并使网络资源的使用达到最优化的程度。

（5）安全管理（security management）：确保网络资源不被非法使用，防止网络资源由于入侵者的攻击而遭到破坏。

2. 网络管理的方式和内容

基于 TCP/IP 的网络管理包括两部分：网络管理站（manager）和被管理的网络单元（被管设备）。这些被管设备的共同点就是都运行 TCP/IP 协议。管理进程和代理进程之间的通信有两种方式：一种是管理进程向代理进程发出请求，询问参数值；另一种方式是代理进程主动向管理进程报告某些重要的事件。

基于 TCP/IP 的网络管理包含 3 个组成部分：

（1）一个管理信息库（Management Information Base，MIB）。管理信息库包含所有代理进程的所有可被查询和修改的参数。

（2）关于 MIB 结构和表示符号——结构管理信息 SMI。例如，SMI 定义计数器是一个非负整数，它的计数范围是 0～4 294 967 295，当达到最大值后，又从 0 开始。

（3）管理进程和代理进程之间的通信协议——简单网络管理协议（Simple Network Management Protocol，SNMP）。SNMP 包括数据交换的格式等，主要采用 UDP 协议。

3. 网络管理的类型与收集数据的方法

网络管理分为两类：

（1）对网络应用程序、用户账号（例如文件的使用）和存取权限（许可）的管理。

（2）对构成网络的硬件，包括工作站、服务器、网卡、路由器、网桥和集线器等的管理。

从被管理设备中收集数据有两种方法：一种是只轮询（polling-only）的方法；另一种是基于中断（interrupt-based）的方法。这两种方法各有利弊，因此它们的结合——面向自陷的轮询方法（trap-directed polling）被认为是执行网络管理最为有效的方法。在这种结合的方法中，当一个设备产生了一个自陷时，就可以使用网络管理工作站来查询该设备（假设它仍然是可到达的），以获得更多的信息。

4. 简单网络管理协议

简单网络管理协议是由 Internet 工程任务组织（Internet Engineering Task Force，IETF）的研究小组为了解决 Internet 上的路由器管理问题首先提出的。但是，SNMP 被设计成与协议无关，所以它可以在 IP、IPX、AppleTalk、OSI 以及其他用到的传输协议上被使用。

SNMP 是一系列协议组和规范，它们提供了一种从网络上的设备中收集网络管理信息的方法，也为设备向网络管理工作站报告问题和错误提供了一种方法。

SNMP 的体系结构分为 SNMP 管理者（SNMP Manager）和 SNMP 代理者（SNMP Agent），每一个支持 SNMP 的网络设备中都包含一个代理，此代理随时记录网络设备的各种情况，网络维护管理程序再通过 SNMP 通信协议查询或修改代理所记录的信息，并把这些数据记录到一个管理信息库（MIB）中。网管员通过向代理的 MIB 发出查询信号可以得到这些信息，这个过程就叫轮询（polling）。为了能全面地查看一天的通信流量和变化率，管理人员必须不断地轮询 SNMP 代理，每分钟就轮询一次。这样，网管员可以使用 SNMP 来评价网络的运行状况，并揭示出通信的趋势，如哪一个网段接近通信负载的最大能力或正使通信出错等。先进的 SNMP 网管站甚至可以通过编程来自动关闭端口或采取其他矫正措施来处理历史的网络数据。

现在，SNMP 已经成为事实上的标准网络维护管理协议。所有的网络公司的产品都宣称自己的产品支持 SNMP 标准，但真正全部具有网络管理五大功能的网络管理系统并不多。具有代表性的国外有 HP 公司的 HP Open View、IBM 公司的 NetView、ZOHO 公司的 ManageEngine、Cisco 公司的 Cisco Works、Sun 公司的 Sun Manager、智和信通公司的 SugarNMS、Novell 公司的 NetWare Manage Wise 和代表未来智能网络管理方向的 Cabletron 公司的 SPECTRUN。这些网管系统在支持本公司网络管理方案的同时，均可通过 SNMP 对网络设备进行管理。还有一些网络公司的网络管理产品基本上都是网络管理代理，可作为 SNMP 代理接受管理者的管理。

5. 网络安全及其管理设备与软件

网络安全是网络管理的重要环节。关于这方面的内容将在第 7 章进行介绍。

实验 2　光纤冷接头制作

一、实验内容

制作光纤尾接头。

二、预备知识

1. 光纤接头及其种类

光纤尾接头（optical fiber splice）是指光纤的末端装置，也称冷接子，用于连接光纤与有关设备。随着光纤技术的广泛应用，光纤接头不断革新，出现了不少品种。按照不同的分类方法，光纤连接器可以分为不同的种类。常用的分类方法有如下几种：

（1）按光纤传输模式，可分为：

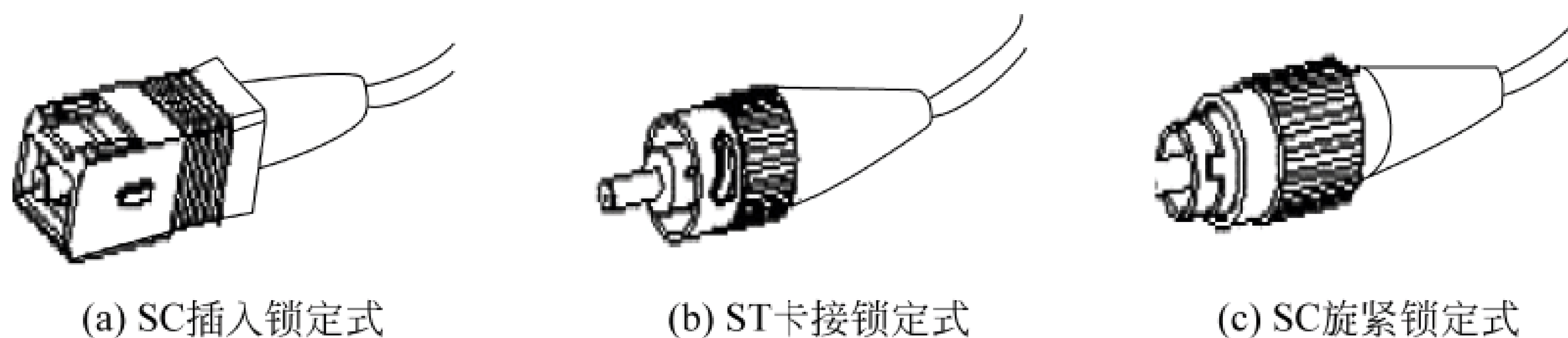
- 单模 L——波长 1310nm，连接距离可达 10km。
- 多模 SM——波长 850nm，连接距离 300m 或 500m。
- 单模长距 LH——波长 1310/1550nm。
- 单模或多模光纤 SX/LH。

（2）按接头外形，可分为：

- 圆头，如 FC、ST 等。
- 方头，如 SC（大方头）、LC（小方头）等。

（3）按紧固方式，有多种，其中常见的是如图 2.16 所示的 3 种。

- 插入锁定式，如 SC 等。
- 卡接锁定式，如 ST 等。
- 旋紧锁定式，如 FC 等。



(a) SC插入锁定式　　(b) ST卡接锁定式　　(c) SC旋紧锁定式

图 2.16　常见的 3 种光纤尾结头

（4）按加固材料，可以分为：

- 金属，如 FC（Ferrule Contactor，钢制金属套筒）、ST 等。
- 工程塑料，如 SC、LC 等。

（5）按连接器的插针端面，主要分为：

- PC（Physical Contact，紧密接触）——微球面研磨抛光。
- SPC（Super Physical Contact，超紧密接触）——球面研磨抛光。
- APC（Angled Physical Contact）——8 度角斜面物理接触，通常为绿色。

注意：在表示尾纤接头的标识符号中，研磨方式 PC、SPC、UPC、APC 写在“/”后面，如 FC/PC、SC/PC 等，“/”前面部分表示尾纤的连接器型号。图 2.17 为三种主要插针端面

形状。



图 2.17　三种主要插针端面形状

（6）按光纤芯数分还有单芯、多芯之分。

（7）按传输速率，分为 1GB（SC）和 2GB（LC）。

表 2.3 为几种主要光线接头的主要特征。

表 2.3　几种主要光线接头的主要特征

型号	外形	加固方式	紧固方式	插针端面	特　点	常用用途
FC	圆形	金属套	螺丝扣	平面/PC	牢固，可多次插拔	ODF 侧(配线架上用的最多)
SC	矩形	工程塑料	插拔销闩式	PC/APC	插拔方便、价格低廉、密度高	传输设备侧（路由器、交换机）
ST	圆形	金属套	螺丝扣		与 SC 现状相似，但略小	设备
MU					以 SC 为基础，体积最小	高密度安装
LC		工程塑料	插孔闩锁		尺寸较小，SFP 模块	路由器
MT-RJ	方形		推拉式插拔			收发一体、高密度传输
DIN4	圆形	金属套	螺丝扣	PC	以 FC 为基础	同 FC

2. 光纤尾接头结构

图 2.18 为 SC 型尾接头结构。

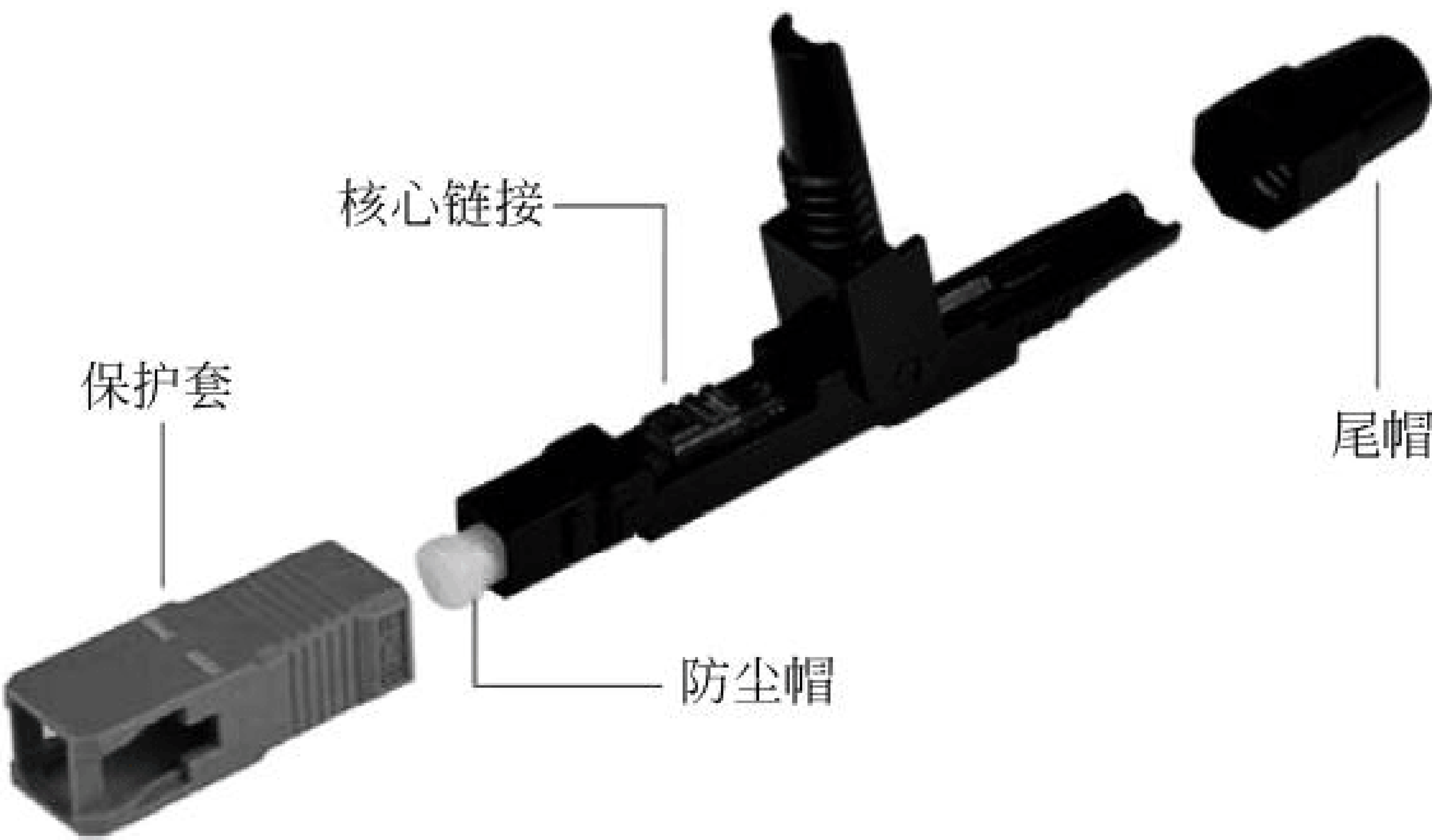


图 2.18　SC 尾接头结构

3. 光纤冷接制作工具

图 2.19 为一组光纤冷接头制作时用到的工具图样。表 2.4 为光纤冷接制作工具一览表。



(a) 光纤皮线开剥器　(b) 光纤切割刀　(c) 米勒钳

(d) 罗宾汉纤维剪刀　(e) 斜口钳　(f) 光纤定长导轨　(g) 笔式红光源

图 2.19　光纤冷接子制作工具

表 2.4　光纤冷接制作工具一览表

序号	工具名称	用　　途
1	光缆皮线开剥器	开剥皮线光缆外护套
2	光纤切割刀	切割光纤纤芯
3	光纤米勒钳	剥离光纤涂覆层/紧包层
4	罗宾汉纤维剪刀	剪切光纤纤维丝用
5	斜口钳	剪线断线用
6	定长开剥器（定长导轨）	开剥线缆及切割纤芯时确定长度
7	笔式红光源 1-5KM	检测光纤断点
8	酒精瓶	盛放酒精，清洁光纤用
9	收纳盒	盛放光纤连接头等小物件

三、注意事项

（1）进行光纤操作时注意环境清洁，防止粉尘烟尘等污染光纤的玻璃颗粒。

（2）安装时施工人员应保持手部清洁干燥，最好戴有干净的乳胶手套。

（3）开剥皮缆线或剥去涂覆层时，要选用正品并保养良好的工具，采用正确的使用方法，减少光纤端面损伤。

（4）定长切割光纤时，要正确使用定长器导轨槽。

（5）插入光纤至连接器，注意操作方法和力度，以免造成断纤。

（6）避免人身伤害，在进行光纤安装操作时必须戴上眼睛保护装置，并且不要用眼睛直接看终端或光纤发出的光线。

（7）切割下的废光纤要非常小心地收集到收纳盒中，这些微小碎片很容易刺伤皮肤。

（8）光纤插入到连接器时，注意操作方法和力度，以免造成断纤。

（9）组装时保持光纤微弯后才能锁紧锁扣。

四、实验准备

1. 工具和材料准备

（1）一段合适长度的试验用光缆。

（2）合适的尾接头一只。

（3）冷接头制作工具一套。

（4）防护眼镜。

（5）工作用橡胶手套一副。

2. 了解尾接头结构

该连接器适用于缓冲层直径为250μm 和900μm的光缆以及外皮直径为2.5～3mm的单芯光缆。对于其他光缆要选择合适的尾接头。

五、冷接子制作参考步骤

线面以SC冷接子为例介绍其制作步骤。

1. 光纤加工

（1）阅读冷接子包装上的使用说明（如图2.20（a）所示），检查与给出的光纤是否匹配。

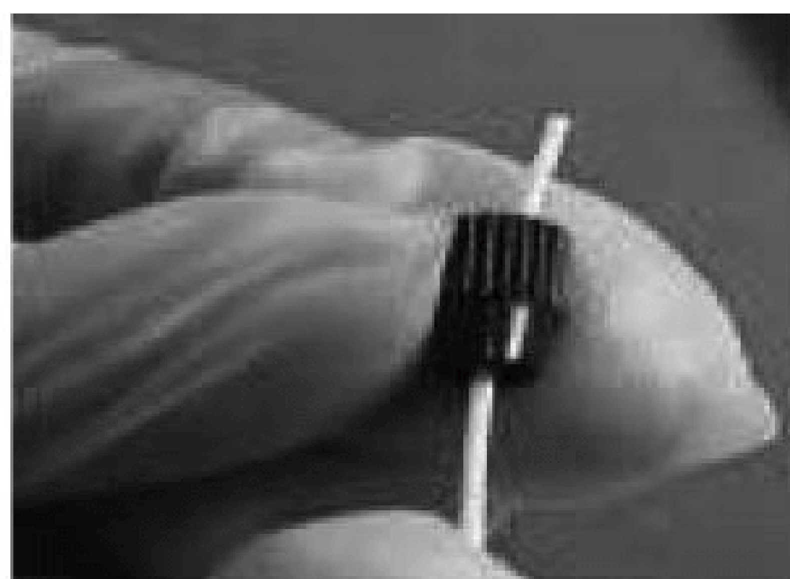
（2）打开冷接子包装，保护好包装。将尾帽小口径的一端朝里套在光缆（光纤的缓冲层）上，如图2.20（b）所示。

（3）如图2.20（c）所示，用皮线剥开器将外护套剥除约50mm（请保留3mm尾纤中的凯夫拉-芳纶并临时向后折）。

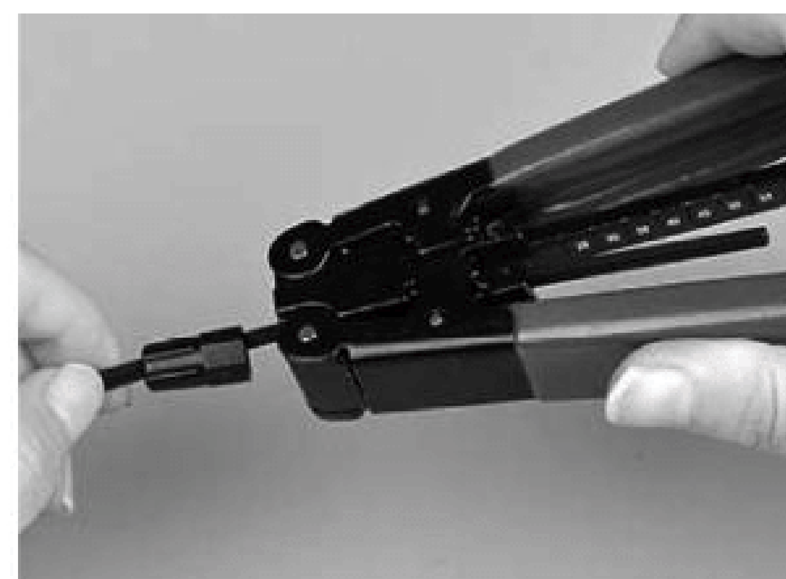
（4）剥除涂覆层，长度按照包装上给出的尺寸进行。例如，包装上要求保留芯线长度24mm，应保留这个长度，将50mm中的其他部分的涂覆层剥除。剥除涂覆层有如下两种方法：



(a) 冷接子包装上的说明



(b) 将尾帽套在光缆上



(c) 把光皮线剥开

图2.20　光缆皮线开剥

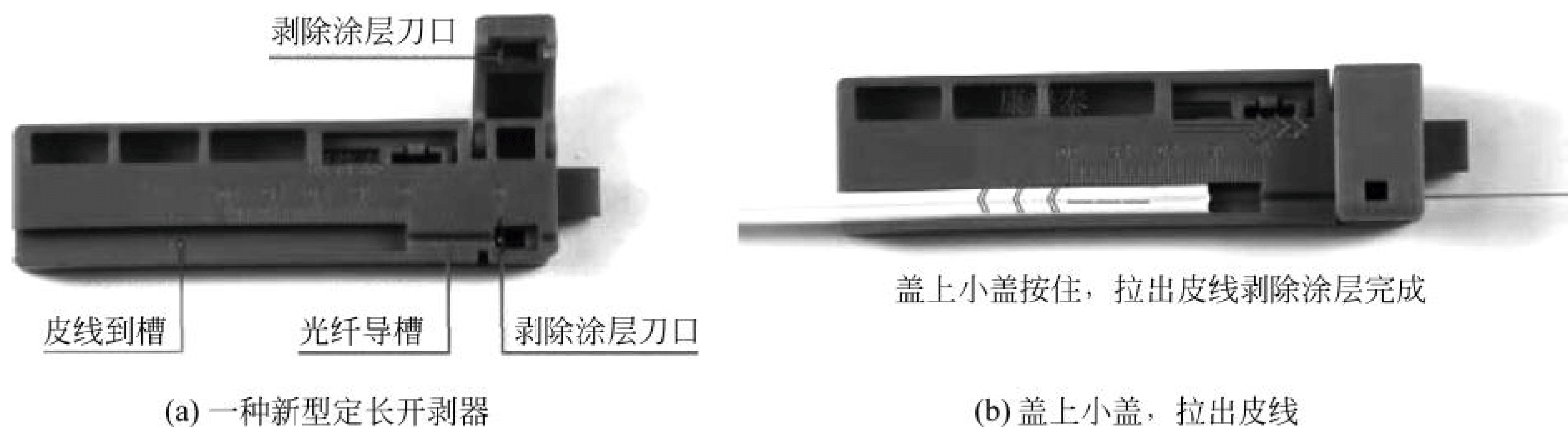
图2.21所示为用米勒钳剥除光纤涂覆层。注意，针对不同用途，有不同的米勒钳，此外按口数有单口、双口和三口之分。例如CFS双扣米勒钳的顶部1.98mm的开孔可用于剥离尾纤外护层，钳刃上的V形口和140μm的开孔可用于剥离125μm光纤的250μm涂覆层。因此米勒钳一定要与所加工的光纤配套，并确认应当使用哪个口。同时，应使钳口与光纤成45°。



图2.21　用米勒钳剥除涂覆层

另一种办法，是使用装有刀片的定长开剥器。这种开剥器一般会有冷接子厂家免费提供。操作分为两步：如图2.22（a）所示，将开剥器打

开，将裸纤放入导槽；如图 2.22（b）所示，然后将开剥器闭合，手指压紧，拉出裸纤，即可剥除涂覆层。



(a) 一种新型定长开剥器　　(b) 盖上小盖，拉出皮线

图 2.22　用定长开剥器剥除涂覆层

（5）用无尘纸或无尘布蘸少许酒精紧贴纤芯擦拭，必要时应重复清洁。

（6）根据包装袋上的图示，保留需要的裸光纤长度，并将纤芯切平。如图 2.23 所示，切割时外护套剥离处要与适配器内底部的标线对齐。

注意：在切平时，要考虑所用的切割刀是否适合所用的切割适配器。例如注意有些切割刀并不适用于 3M 切割适配器。有时这一步可以直接把光纤放入切割刀进行切割。



图 2.23　切平光纤

2. 冷接子装配

装配过程如图 2.24 所示。



(a) 插入光缆(光纤)　　(b) 插至光纤弯曲，确定光纤插入到位

(c) 用手压紧光缆，先推外壳再推紧锁扣　　(d) 取下锁扣，保持光纤微弯

(e) 确认对接正常，否则重复步聚(c)　　(f) 旋紧尾套，完成安装

图 2.24　冷接子装配

3. 测试

最简单的测试是用笔式红光源从光纤一段照进，让另一端照在纸或其他地方（但不要用眼睛看），就可以检测出是否接通。

六、分析与讨论

（1）为什么光纤最后要切平？
（2）为什么光纤插入连接器时，要插到光纤微弯曲？

实验 3 安 装 网 卡

一、实验内容

本实验进行以太网网卡安装训练。

二、材料和工具准备

（1）一块合适的以太网网卡。
（2）一把合适的螺丝刀。

三、实验参考步骤

1. 安装网卡硬件
（1）在计算机处于关闭状态下，拔下电源插头。
（2）打开机箱，为网卡寻找合适的插槽（如果是 PCI 网卡则选择 PCI 插口）。
（3）用螺丝刀卸下下插槽后面挡板上的防尘片，露出条形窗口。
（4）将网卡垂直插入插槽，使有接头的一侧面向机箱后侧。
（5）将网卡的金属接头挡板用螺丝固定在条形窗口顶部的螺丝孔上。
（6）盖上机箱，拧好固定螺丝，硬件安装完成。
注意： 对于 USB 网卡和 PCMCIA 网卡（笔记本专用），不需要拆卸机箱。
2. 安装网卡驱动程序

计算机每安装一种硬件，都需要相应的驱动程序才能正常使用。Windows 2000 以上的操作系统已经集成了多种驱动程序。如果系统没有携带某种硬件的驱动程序，那么启动安装好网卡硬件的机器，Windows 会自动检测新增硬件，并启动添加新硬件向导，引导用户安装驱动程序。

打开计算机，操作系统会检测到网卡并提示用户插入驱动程序盘。插入随网卡销售的驱动程序盘，然后按照向导的引导单击“下一步”按钮，直到找到驱动程序，单击“完成”按钮。

四、附加实验

在笔记本上安装 PCMCIA 网卡，并安装网卡驱动程序。

五、分析与讨论

（1）如何挑选网卡？
（2）为什么安装了网卡硬件后还要安装网卡驱动程序？

实验 4　用 Hub 组建对等网

一、实验内容

用 Hub 组建 10/100BAST 网络。

二、实验准备

（1）已经安装有 10/100Mbps 网卡的计算机 3 台以上。
（2）与计算机数量相同的直通网线。
（3）一台有 8 个以上端口的 Hub。

三、预备知识

对等网也称为工作组，是一种比较小而简单的网络。在对等网中，各台计算机有相同的地位，无主次之分，既可以向别的计算机提供信息服务，也可以得到其他计算机提供的信息服务。与对等网对应的网络是工作站-服务器网络。按照工作站-服务器的概念，对等网中的每一台计算机既充当工作站的角色，又充当服务器的角色。

四、实验参考步骤

（1）检测网线是否正确。
（2）检测 Hub 是否能正常工作。
（3）关闭计算机的电源，用 Hub 将计算机连接成一个小型以太网。
（4）启动计算机，打开“网上邻居”，用下面的一种方法查看本组计算机的连接情况：
- 双击“邻近的计算机”图标；
- 双击“整个网络”图标。

五、附加实验

为自己或他人组建一个对等式局域网。

六、分析与讨论

（1）为什么连接网络之前要先关闭欲连接计算机的电源？
（2）记录组网过程中出现的不正常现象，并分析出现的原因。

实验 5　交换机的基本配置

一、实验目的

掌握交换机安装和配置的基本方法。

二、实验内容

（1）熟悉交换机的接口及其接线方法，弄清各指示灯的基本含义。
（2）熟悉交换机的基本配置命令。

三、器材准备

（1）思科 2950T 交换机一台及随机附带的控制台专用线一根。
（2）装有网卡和 Windows 2000（操作系统）的计算机一台。
（3）装有以太网卡的计算机及双绞线若干。

四、实验参考步骤

1. 了解交换机外部结构和功能

思科 2950T 交换机的前面板部分包括 24 个 10/100Mbps 端口、电源指示、连接状态指示灯、10/100Mbps 状态指示灯，全/半双工及冲突指示灯。各接口分布如图 2.25 所示。

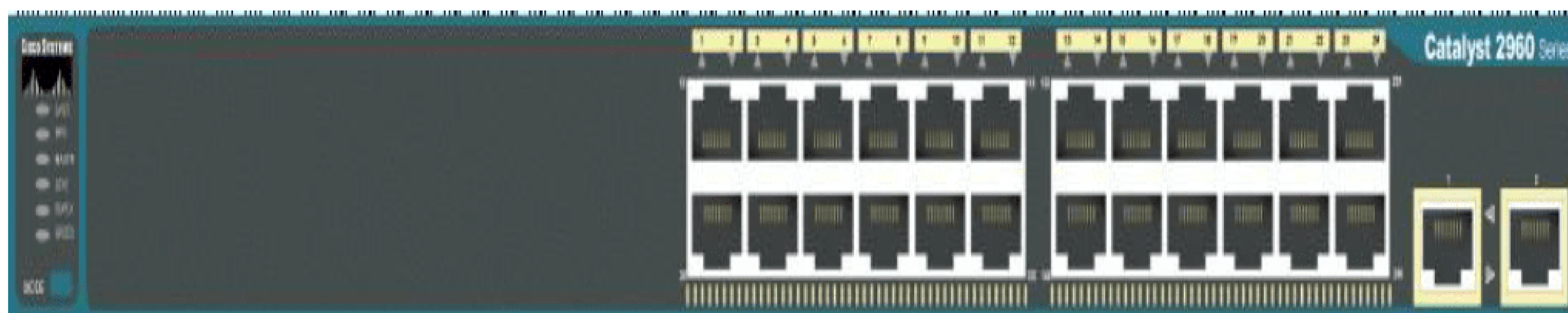


图 2.25　思科 2950T 交换机前面板

2. 常用配置命令

如图 2.26 所示，将计算机与交换机连接好。

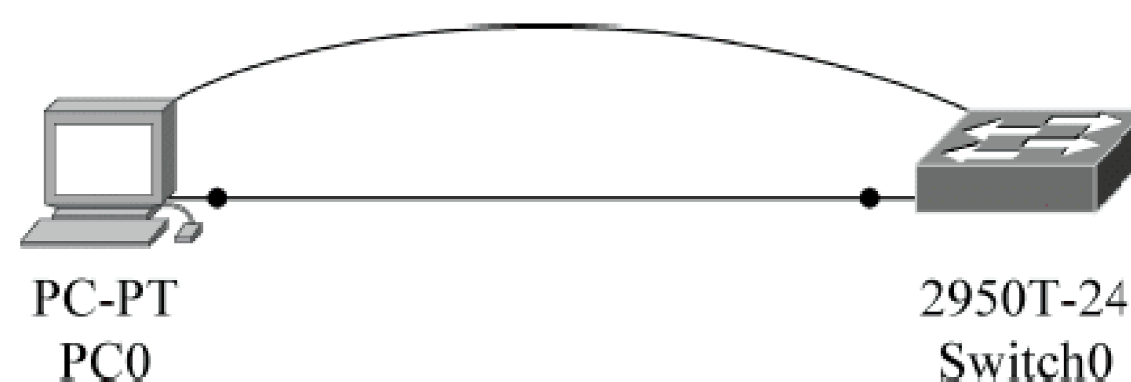


图 2.26　计算机与交换机的连接方式

1）常见的几种命令模式

```
switch>(用户命令模式，只能使用一些查看命令)
switch#(特权命令模式)
switch(config)#(全局配置模式)
switch(config-if)#(端口配置命令模式)
```

各种配置模式间的关系如下：

```
Switch>                                   //用户模式
Switch>enable                             //进入特权模式
Switch#disable                            //退回用户模式
Switch#configure terminal                 //进入配置模式
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CoreSW            //更改主机名
CoreSW(config)#interface f0/1             //进入端口模式
CoreSW(config-if)#
```

2）检查、查看命令

这些命令用于查看当前配置状况，通常是以 show（sh）为开始的命令。show version 可查看 IOS 的版本，show flash 可查看 flash 内存使用状况，show mac-address-table 可查看 MAC 地址列表。

```
CoreSW#show version                   //显示 IOS 版本号
CoreSW#show flash                     //查看 flash 内存使用状况
CoreSW#show mac-address-table         //查看 MAC 地址列表
CoreSW#show ?                         //帮助显示所有的查看命令
  arp                    Arp table
  boot                   show boot attributes
  cdp                    CDP information
  clock                  Display the system clock
  dtp                    DTP information
  flash:                 Display information about flash: file system
  history                Display the session command history
  hosts                  IP domain-name, lookup style, nameservers, and host table
  interfaces             Interface status and configuration
  ip                     IP information
  mac-address-table      MAC forwarding table
  port-security          Show secure port information
  processes              Active process statistics
  running-config         Current operating configuration
  sessions               Information about Telnet connections
  spanning-tree          Spanning tree topology
  startup-config         Contents of startup configuration
  tcp                    Status of TCP connections
  terminal               Display terminal configuration parameters
  users                  Display information about terminal lines
  version                System hardware and software status
  vlan                   VTP VLAN status
  vtp                    VTP information
CoreSW#show              interface fa0/1 //查看端口状态信息
```

3）密码设置命令

Cisco 交换机、路由器中有很多密码，设置好这些密码可以有效地提高设备的安全性。

```
switch(config)#enable password   //设置进入特权模式的密码
```

```
switch(config-line) #          //可以设置通过 console 端口连接设备及 telnet 远程登录时所需要的密码
```

配置路由器的登录密码和远程登录密码：

```
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#enable password able
CoreSW(config)#line console 0
CoreSW(config-line)#password line
CoreSW(config-line)#login
CoreSW(config-line)#line vty 0 4
CoreSW(config-line)#password vty
CoreSW(config-line)#login
CoreSW(config-line)#exit
CoreSW(config)#
```

以上是设置交换机的各种密码。默认情况下，这些密码都是以明文的形式存储，所以很容易查看到。

4）配置 IP 地址及默认网关

```
CoreSW(config)#interface vlan1
CoreSW(config-if)#ip address 192.168.0.253 255.255.255.0
CoreSW(config-if)#exit
CoreSW(config)#ip default-gateway 192.168.0.1
```

5）管理 MAC 地址表

```
switch#show mac-address-table                // 显示 MAC 地址列表
switch#clear mac-address-table dynamic       // 清除动态 MAC 地址列表
CoreSW#show mac-address-table                // 显示 MAC 地址列表
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

设置端口的静态 MAC 地址，将端口 fa0/1 的 MAC 地址设为 001122335588。

```
CoreSW(config)#mac-address-table static 0011.2233.5588 vlan 1 interface fa0/1
CoreSW(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
CoreSW#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0011.2233.5588    STATIC      Fa0/1
```

每个端口对应一组优先级，选择相应端口的优先级，单击“确定”按钮，完成优先级

的设置。

五、附加实验

试修改交换机的主机名和登录密码。

习　题　2

一、选择题

1．下列传输介质中，抗干扰能力最强的是【　　】。

A．双绞线　B．超五类双绞线　C．电磁波　D．光缆

2．下列传输介质中，带宽最宽、信号传输衰减最小、抗干扰能力最强的是【　　】。

A．微波　B．双绞线　C．同轴电缆　D．光纤

3．下列选项中，不属于有线传输介质的是【　　】。

A．红外线　B．双绞线　C．同轴电缆　D．光纤

4．在常用的网络传输介质中，【　　】具有更好的技术性能。

A．双绞线　B．同轴电缆　C．光纤　D．无线信道

5．网卡实现的是OSI/RM中【　　】的功能。

A．物理层和数据链路层　B．物理层、数据链路层和网络层

C．运输层和网络层　D．应用层和网络层

6．中继器的作用是【　　】。

A．将信号放大、整形和转发　B．将信号放大、整形并选择路径转发

C．扩展网络的传输距离　D．让所有链路共享带宽

7．10Mbps和100Mbps自适应系统是指【　　】。

A．既可工作在10Mbps，也可工作在100Mbps

B．既工作在10Mbps，同时也工作在100Mbps

C．端口之间10Mbps和100Mbps传输率的自动匹配功能

D．以上都是

8．路由就是网间互联，其功能是发生在OSI参考模型的【　　】。

A．物理层　B. 数据链路层　C. 网络层　D. 以上都不是

9．下列不属于通信设备的是【　　】。

A．路由器　B．交换机　C．调制解调器　D．集线器

10．需要将一个局域网分为多个IP子网，应当选用的网络互联设备是【　　】。

A．路由器　B．交换机　C．麦克风　D．集线器

11．下列设备中，可以控制广播数据传输的是【　　】。

A．路由器　B．交换机　C．调制解调器　D．集线器

12．下列设备中，不属于网络连接设备的是【　　】。

A．路由器　B．交换机　C．视频卡　D．集线器

13．现在常用的网络操作系统是【　　】。

A．Windows 2000和UNIX　　B．Windows 2000和Web

C．Windows 2000和IE8　　D．Windows 2000和IP

14．下列选项中，不属于网络操作系统的是【　　】。

A．Windows 2003　　B．Linux　　C．UNIX　　D．Windows 98

二、填空题

1. 3类双绞线与5类双绞线比，绞绕密度高的是______________ 。
2．光纤从内到外，依次是__________、__________、__________、缓冲层和_________。
3. 电力线载波是把____________加载于____________用____________传输，接收信息的适配器再把________________分离出来并传送到计算机或电话以实现信息传递。
4. 无线传输是利用____________携带___________进行的数据传输。
5. 无线传输可以被分为_____________和_____________两大类。
6. VLC是利用荧光灯或发光二极管等发出的肉眼看不到的____________________来携带数据进行传输。
7. 每个网卡都有一个编码。这个编码由____________和______________两部分组成，每一部分为___________进制码，每组__________，用__________分隔。__________就将此作为设备的MAC地址。
8. 集线器的主要作用是____。
9. 交换机的转发依据是__________，路由器的转发依据是_____________。

三、简答题

1. 简述网卡的工作原理。
2. 简述集线器的工作原理。
3. 简述交换机的工作原理。
4. 简述路由器的工作原理。

第 3 章　TCP/IP 与网络互连

TCP/IP 协议栈可以分为应用层、传输层、网际层和网络接口层 4 层。其核心是 TCP/IP。本章从应用的角度，介绍它们的细节，并将之分为 TCP/UDP、IP、ICMP、路由协议和网络接口 5 部分。图 3.1 为对于图 1.55 的细化。

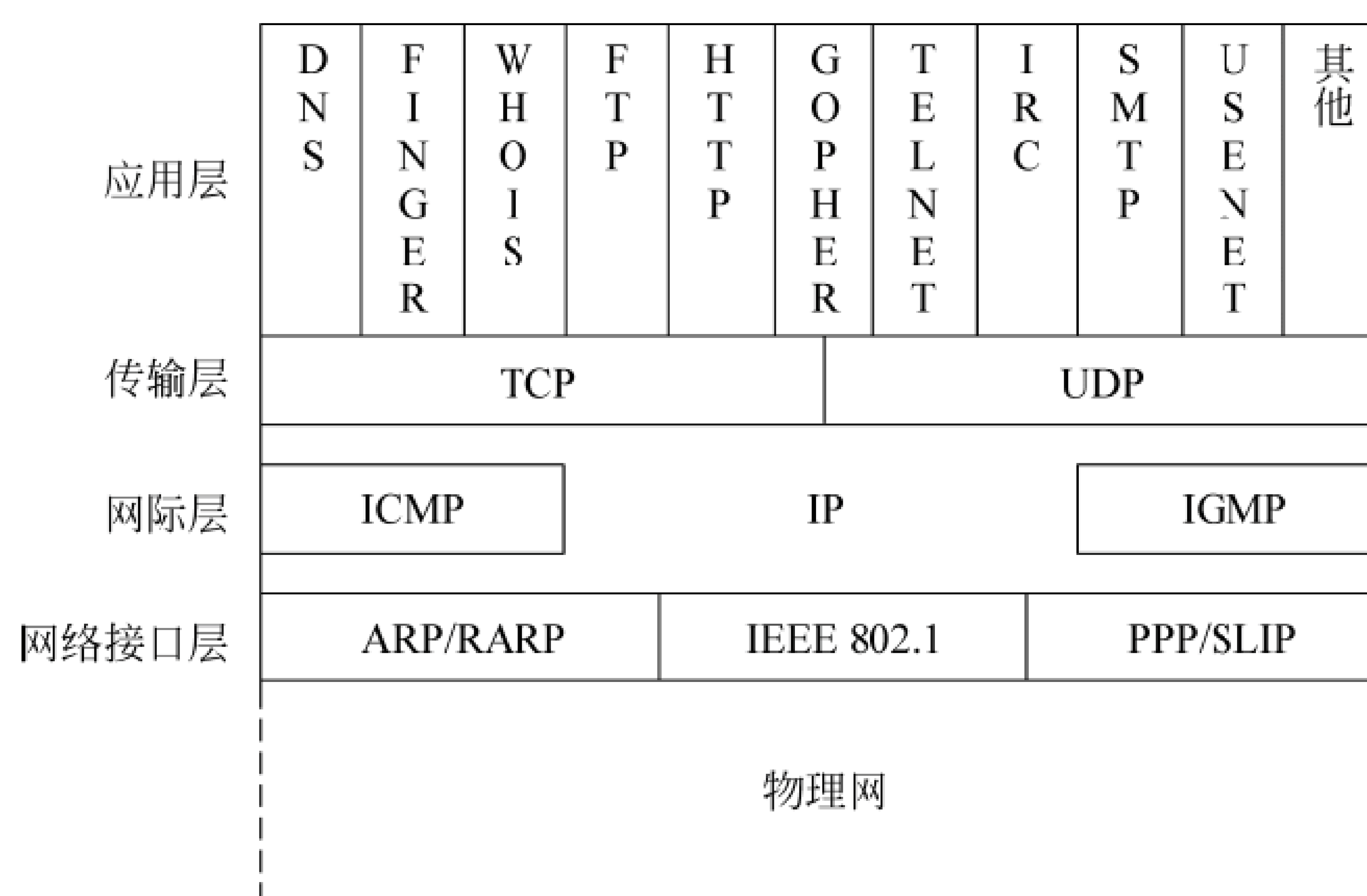


图 3.1　细化的 TCP/IP 参考模型

传输层和 IP 层是 TCP/IP 体系的核心，也是本章的主要内容。图 3.2 为它们在 TCP/IP 体系中的位置和基本职责：传输层提供应用进程之间的逻辑通信，IP 层提供互联网络中两台主机之间的通信，尽最大努力为传输层提供服务。

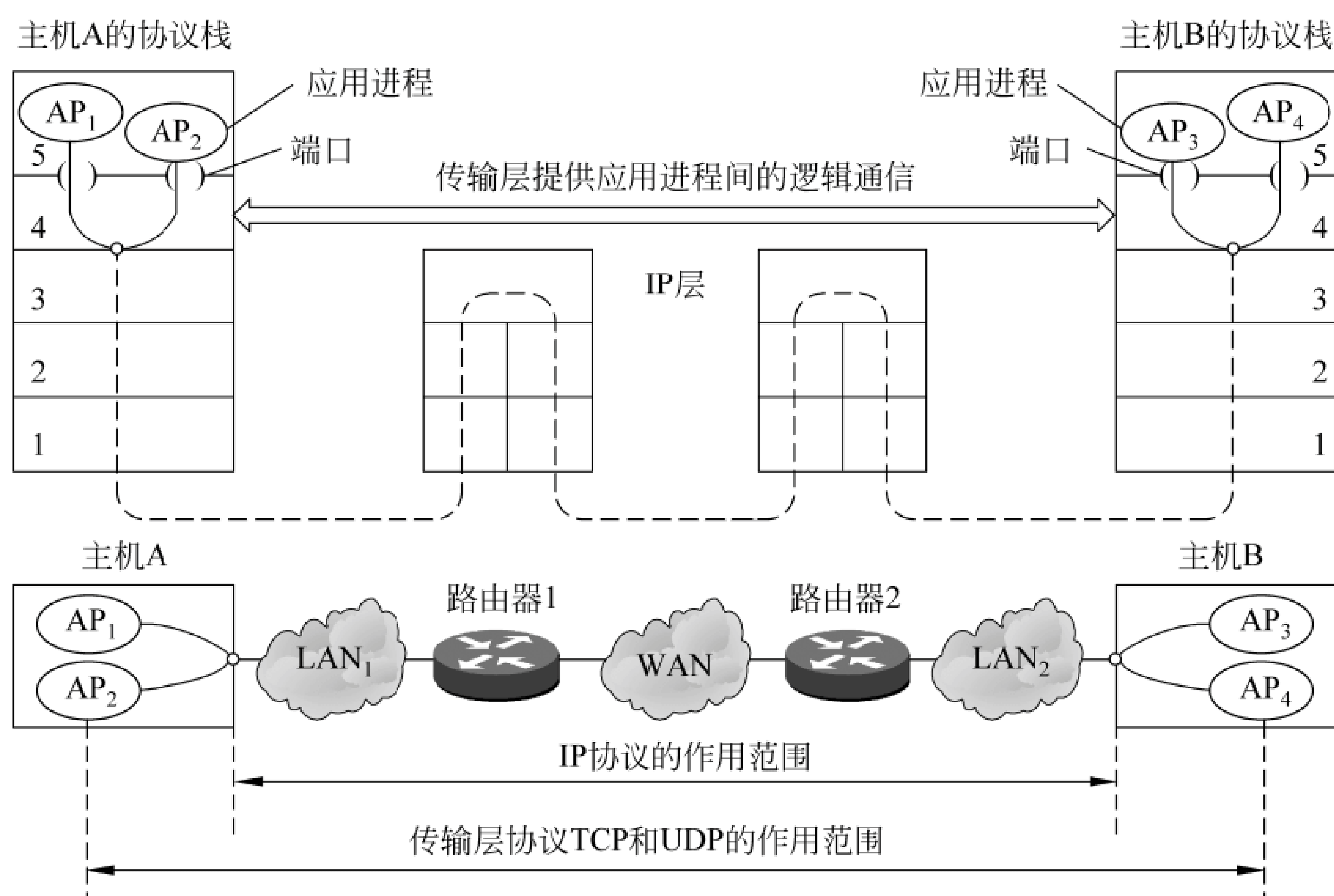


图 3.2　TCP/IP 体系中的传输层与 IP 层模型

3.1　TCP/UDP 协议

在 TCP/IP 网络体系中，TCP/UDP 层是应用层与通信子网之间的接口。它将应用层的数据提交到网络上，并抽象为进程之间的端到端的传送。这种端到端的传输具有 3 个重要特征：

（1）应用层的应用进程很多，为了区分不同的应用进程，在传输层使用了端口（port）的概念。用端口号区分和识别不同的应用协议。

（2）为了在网络上有效地传输，在传输层将对应用层报文进行分段，并形成两种传输模式：TCP（Transmission Control Protocol，运输控制协议）和 UDP（User Datagram Protocol，用户数据报协议）。TCP 是建立在虚电路基础上的有连接端对端可靠传输，UDP 是建立数据报基础上的无连接端对端传输。

（3）如图 3.3 所示，在传输层具有多路复用功能。

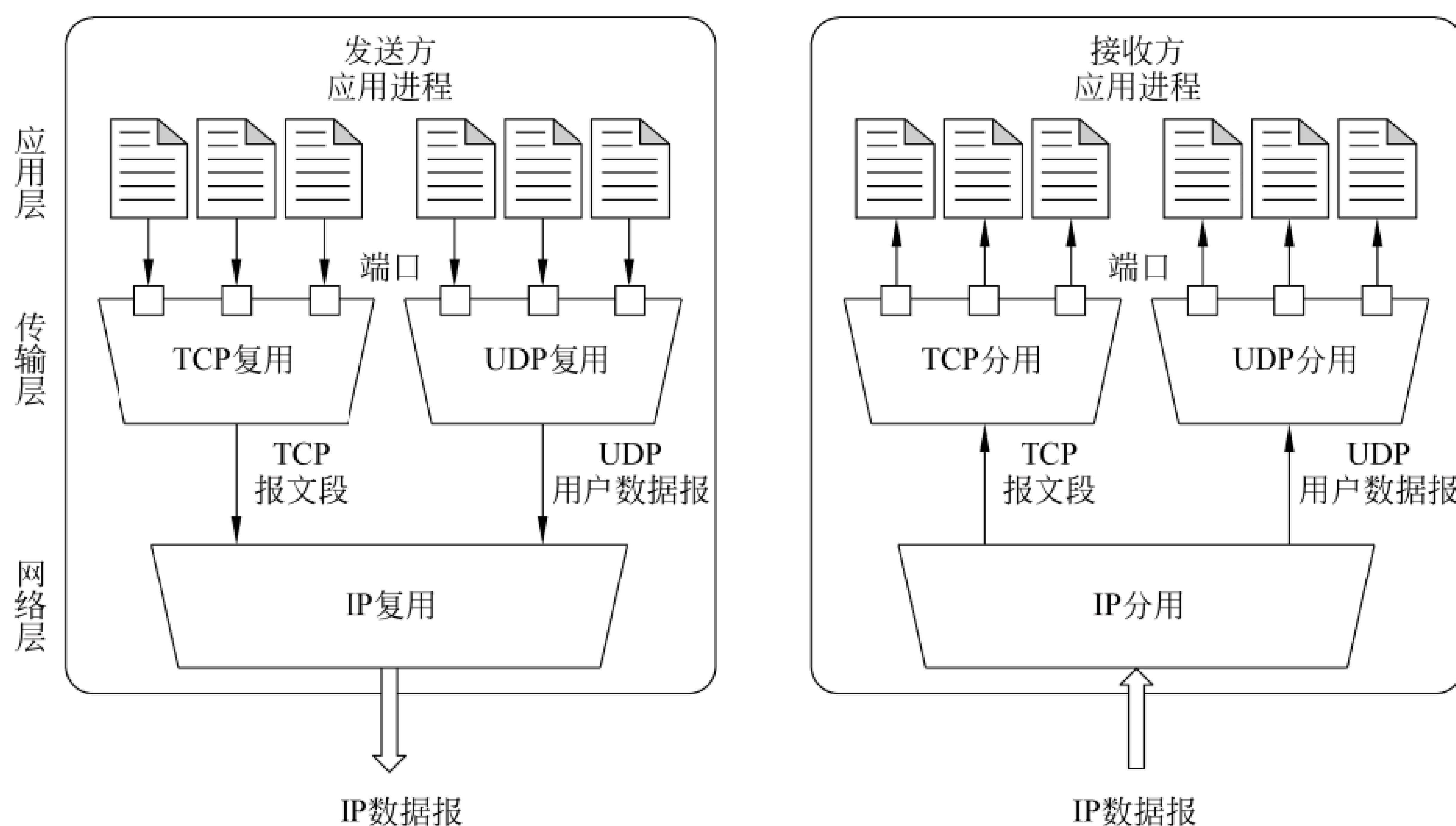


图 3.3　TCP 与 UDP

3.1.1　协议端口

传输层是网络中非常关键的一层。传输层的下面是网络级通信，传输层上面是主机级通信，即进程级通信。由于每个进程都与一个相应的应用协议相联系，因此 TCP/UDP 协议簇中使用 2B 协议端口号（通常也简称端口号）来标识一台机器上的多个进程。端口可以分为 3 大类。

1. 公认端口

公认端口（well known ports）也称为统一分配（universal assignment）端口、众所周知端口和保留端口，是由中央管理机构用静态方式分配的端口号。这些端口号是固定的、全局性的，所有采用 TCP/IP 协议的标准服务器都必须遵从。TCP 与 UDP 的标准端口号是各

自独立编号的，范围在 0～1023 之间。

2. 注册端口

注册端口（registered ports）号在 1024～49 151。它们松散地绑定于一些服务上，多数没有明确地定义服务对象，不同程序可以根据需要自己定义，向 IANA 注册。

3. 动态和/或私有端口

这类端口（dynamic and/or private ports）在 49 152～65 535 之间，可以临时顶替某些端口，以免与别的同协议进程冲突。

表 3.1 列出了一些当前分配的 TCP 和 UDP 的端口号。

表 3.1　一些当前分配的 TCP 和 UDP 的协议端口号

端口号	关　键　字	UNIX 关键字	说　　明	UDP	TCP
7	ECHO	echo	回显		Y
13	DAYTIME	daytime		Y	Y
19	CHARACTER GENERATOR	Character generator		Y	Y
20	FTP_DATA	ftp_data	文件传输协议（数据）		Y
21	FTP_CONTRAL	ftp	文件传输协议（命令）		Y
22	SSH	ssh	安全命令解释程序		Y
23	TELNET	telnet	远程连接		Y
25	SMTP	smtp	简单邮件传输协议		Y
37	TIME	time	时间	Y	Y
42	NAMESERVER	name	主机名服务器	Y	Y
43	NICNAME	whois	找人	Y	Y
53	DOMAIN	nameserver	DNS（域名服务器）	Y	Y
69	TFTP	tftp	简单文件传输协议	Y	
70	GOPHER	gopher	Gopher		Y
79	FINGER	finger	Finger		Y
80	WWW	www	WWW 服务器		Y
101	HOSTNAME	hostname	NIC 主机名服务器		Y
103	X400	x400	X.400 邮件服务		Y
104	X400_SND	x400_snd	X.400 邮件发送		Y
110	POP3	pop3	邮局协议版本 3		Y
111	RPC	rpc	远程过程调用	Y	Y
119	NNTP	nntp	USENET 新闻传输协议	Y	Y
123	NTP	ntp	网络时间协议	Y	Y
161	SNMP	snmp	简单网络管理协议	Y	
179	BGP		边界网关协议		Y
520	RIP		路由信息协议	Y	

3.1.2　TCP 的特征

TCP 是传输层的一个主要协议，从应用程序的角度看，TCP 提供的服务具有如下特征。

1．端对端的通信

TCP 是在网络层提供的服务基础上，提供一个直接从一台计算机上的应用到另一台远程计算机上的应用的连接。由于每一个 TCP 连接都有两个端点，所以是一种端对端的协议。

2．虚电路连接

TCP 提供面向连接的服务，其传输过程由 3 个过程组成：建立连接、传输数据和释放连接。即一个应用程序必须首先请求一个到目的地的连接，然后才能使用该连接传输数据。由于该连接是通过软件实现的，所以是虚连接（virtual connection）。

3．全双工通信

一个 TCP 连接允许任何一个应用程序在任何时刻发送数据，使数据在该 TCP 的任何一个方向上流动，并可以在传输数据包时搭载应答信息。

4．可靠传输

（1）可靠连接。指防止在连接过程一方要发送数据而另一方还没有做好准备。

（2）确认和超时重传机制。TCP 在发送一段报文时，要同时在自己一侧存放该报文的一个副本。若收到确认，则删除该副本；若在超时之前没有收到确认，则重传该报文段。

（3）字节编号。TCP 协议是面向字节的，它将所要传送的报文看成字节流。为了对字节的确认，需要为每个字节提供一个编号（在数据链路层中是为帧进行编号）。另外，字节序号并不是从 0 或 1 开始的。初始的序号是通信开始时双方商定的。并且，TCP 接收方送给发送方的确认是接收到的最后一个序号+1——期待接收的数据的编号，即前面的字节都已经正确收到。例如，接收端已经正确地接收到了 201~300 号字节的数据，则发给对方的确认号为 301，表示等待 301 号字节到来。

（4）校验和。TCP 采用校验和进行检错。这种方法检错能力不强，但效率比较高，符合 TCP/IP 的设计原则。同时，随着低层网络质量的改善，这种方法也能达到要求。

（5）从容关闭。从容关闭是指确保关闭连接之前传递完所有的数据。

5．基于滑动窗口的流量控制和拥塞控制

当建立一个 TCP 连接时，连接的每一端分配一个缓冲区来保存输入的数据。通常把缓冲区中的空闲部分称为窗口。TCP 采用可变滑动窗口协议，并且当交付的数据不够填满一个缓冲区时，应用程序可以用流服务提供的“推（push）”机制进行强迫传送。

3.1.3　TCP 报文格式

TCP 的报文段由首部和数据部两部分组成。图 3.4 为 TCP 报文段的首部格式。TCP 的数据部为应用层报文。

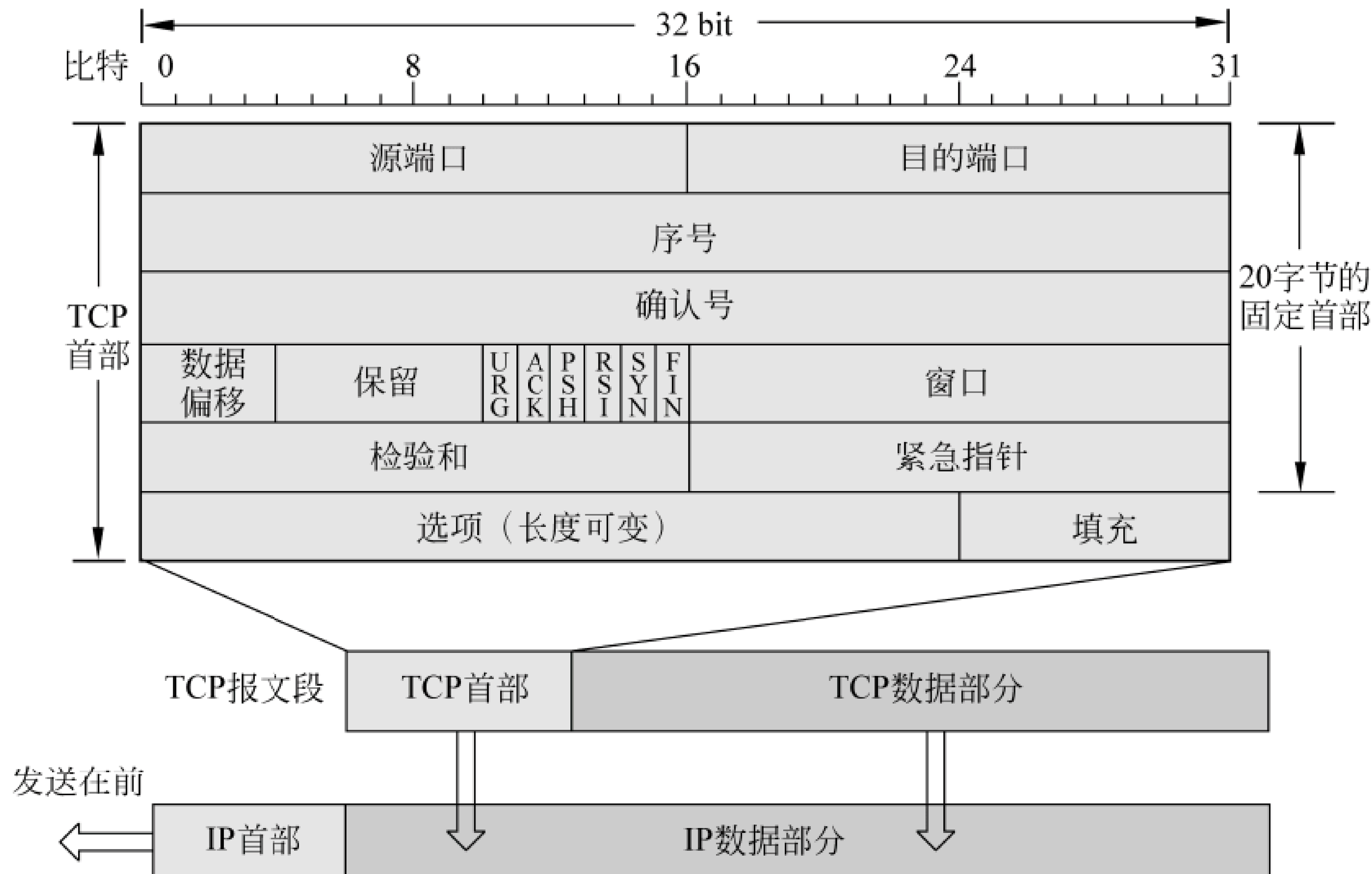


图 3.4　TCP 报文段格式

下面分别介绍各字段的含义。

1）源端口（Source Port）

源端口即本地通信端口，支持 TCP 的多路复用机制。

2）目的端口（Destination Port）

目的端口即远地通信端口，支持 TCP 的多路复用机制。

3）序号（Sequence Number）

序号是数据段的第 1 个数据字节（除含有 SYN 的段外）的序号。在 SYN 段中，该域是 SYN 的序号，即建立本次连接的初始序号，在该连接上发送的第 1 个数据字节的序号为初始序号+1。

4）数据偏移（Data Offset）

数据偏移指出该段中数据的起始位置，以 4 字节为单位（TCP 头总以 32 位边界对齐）。

5）6 个控制位（Control Bit）

URG——紧急指针域有效。URG=1 表示该段中携带有紧急数据。

ACK——ACK=1，确认序号有效；ACK=0，确认序号无效。

RST——连接复位，RST=1 表示 TCP 连接中出现严重差错，必须释放连接。

SYN——建立连接时用来同步序号：SYN=1，ACK=0，表明这是一个连接请求报文段；SYN=1，ACK=1，表明这是一个连接请求或连接请求接受报文段。

FIN——发送方字节流结束。FIN=1 表明本端数据已经发送完，请求释放连接。

PSH——本报文段请求“推（push）”操作。即认定该段为“推进”段，段中数据是发送方当时发送缓冲区中的全部数据。对于收到这种数据的接收方来讲，应当把“推进”段

中的数据尽快交给用户，并结束一次用户接收请求。

6）确认号（Acknowledgment Number）

当 TCP 段头控制位中的 ACK 置位时，确认号才有效。它表示本地希望接收的下一个数据字节的序号。对于收到有效确认号的发送者来说，其值表示接收者已经正确接收到了该序号以前的数据。

7）窗口（Window）

表明该段的接收方当前能够接收的从确认号开始的最大数据长度，该值主要向对方通告本地接收缓冲区的使用情况。

8）校验和（Checksum）

校验对象包括协议伪头、TCP 报头和数据。

9）选项（Option）

选项位于 TCP 头的尾端，有单字节和多字节两种格式。单字节格式只有选项类型；多字节格式由一个字节的选项类型、多字节的实际选项数据和一个字节的选项长度（三部分的长度）组成。下面说明 TCP 协议必须实现的选项。

（1）选项表尾选项：KIND=0。表示 TCP 头中由全部选项组成的选项表结束。其格式为：

0	0	0	0	0	0	0	0

（2）无操作选项：KIND=1。该选项可能出现在两个选项之间，作为一个选项分隔符，或提供一种选项字边界对齐的手段，本身无任何意义。其格式为：

0	0	0	0	0	0	0	1

（3）最大段长选项：KIND=2，LENGTH=4。该选项主要用于通知通信连接的对方本地能够接收的最大段长。它只出现在 TCP 的初始建链请求中（SYN 段）。如果在 TCP 的 SYN 段中没有给出该选项，就意味着有能力接收任何长度的段。其格式为：

0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	最大段长

10）填充（Padding）

当 TCP 头由于含有了选项而无法以 32 位边界对齐时，将会在 TCP 头的尾部出现若干字节的全 0 填充。

11）URG 位和紧急指针（Urgent Pointer）

传输层协议使用带外数据（Out-Of-Band，OOB）机制来传输一些重要数据，如通信的一方有重要的事情通知对方，需要加速传送这些通知数据。TCP 支持一个字节的带外数据，并提供了一种紧急模式：在数据分组中设置 URG = 1，表示进入紧急模式，同时用紧急指针表明从该段序号开始的一个正向位移，指向紧急数据的最后一个字节。

3.1.4　TCP 的可靠连接与从容关闭

TCP 是一种面向连接的协议，所以其传输过程由 3 个过程组成：建立连接、传输数据和释放连接。

1. TCP 的可靠连接

TCP 的建立应当是可靠的。TCP 建立可靠连接的方法是采用三次握手（three-way handshaking）方法。握手也称联络，是在两个或多个网络设备之间通过交换报文序列以保证传输同步的过程。如图 3.5 所示为用三次握手方式建立 TCP 连接的过程。

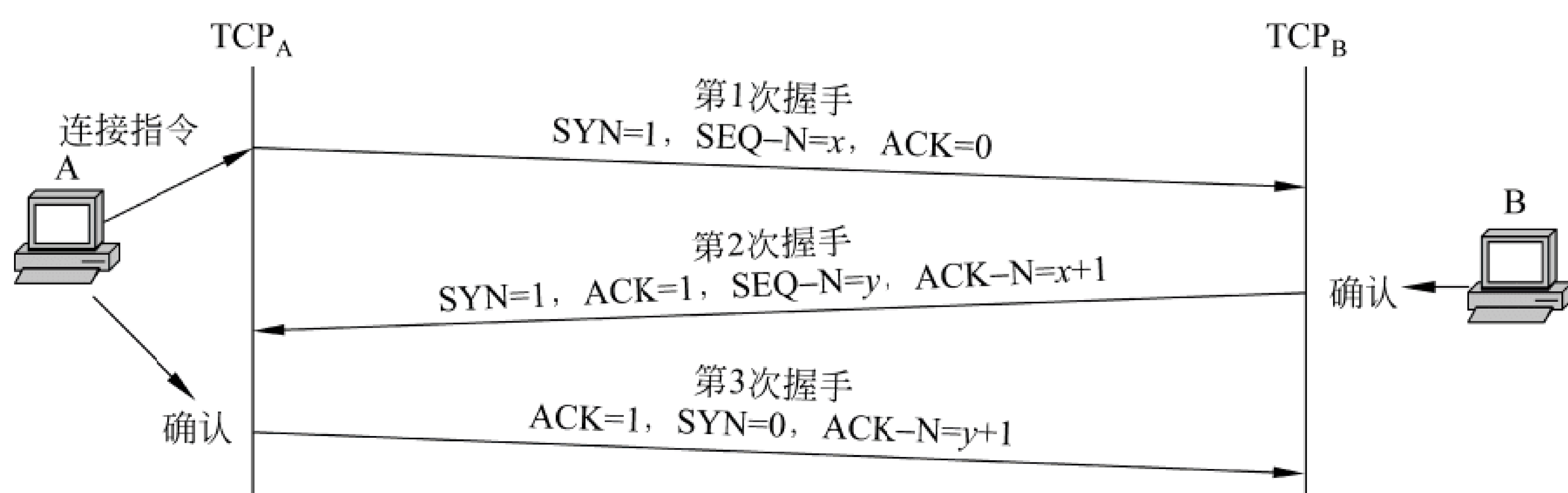


图 3.5　三次握手建立可靠 TCP 连接的过程

第 1 次握手：主机 A 发出主动打开（active open）命令，TCP_A 向 TCP_B 发出请求报文，内容如下。

- SYN=1，ACK=0：表明该报文是请求报文，不携带应答。
- SEQ–N= x：自己的序号为 x，后面要发送的数据序号为 x+1。

第 2 次握手：TCP_B 收到连接请求后，如同意连接，则发回一个确认报文，内容如下。

- SYN=1，ACK=1：该报文为接收连接确认报文，并携带有应答。
- ACK–N = x + 1：确认了序号为 x 的报文，期待接收序号以 x + 1 为第一字节的报文。
- SEQ–N = y：自己的序号为 y，后面要发送的数据序号为 y + 1。

这时，TCP_A 和 TCP_B 会分别通知主机 A 和主机 B，连接已经建立。

到此为止，似乎就可以正式传输数据报文了。但是，问题没有这么简单。因为虽然 B 端同意了接收由 TCP_A 发起的连接，准备好了接收由 TCP_A 发来的数据，而 A 端还没有同意由 TCP_B 发起的连接。所以这时的连接仅仅是全双工通信中的半连接——TCP_A 到 TCP_B 的连接，TCP_B 到 TCP_A 连接并没有建立起来。

所以，只有两次握手的连接是不可靠的。为了避免这种情况，必须再来一次握手。

第 3 次握手：TCP_A 收到含两次初始序号的应答后，再向 TCP_B 发一个带两次连接序号的确认报文，内容如下。

- ACK=1，SYN=0：该报文是单纯的确认报文，但不携带要传输数据的序号。
- ACK–N = y+1：确认了序号为 y 的报文，期待第 1 字节序号为 y + 1 的数据字段。

这样，双方才可以开始传输数据，并且不会出现前面的问题了。

经过三次握手，已经实现了可靠连接的双方就可以传输数据了。下面介绍数据传输过程中的一些关键技术。

2. TCP 连接的从容关闭

TCP 连接是在硬件连接的基础上通过软件实现的，所以称为软连接。软连接后就要占用硬连接的资源。连接释放就是释放一个 TCP 连接所占用的资源。

正常的释放连接是通过断连请求及断连确认实现的。但是，在某些情况下，没有经过断连确认，也可以释放连接，但断连不当就有可能造成数据丢失。如图 3.6 所示为一种断连不当引起数据丢失的情形：A 方连续发送两个数据后，发送了断连请求；B 方在收到第一个数据后，先发出了断连请求，结果第二个数据丢失。

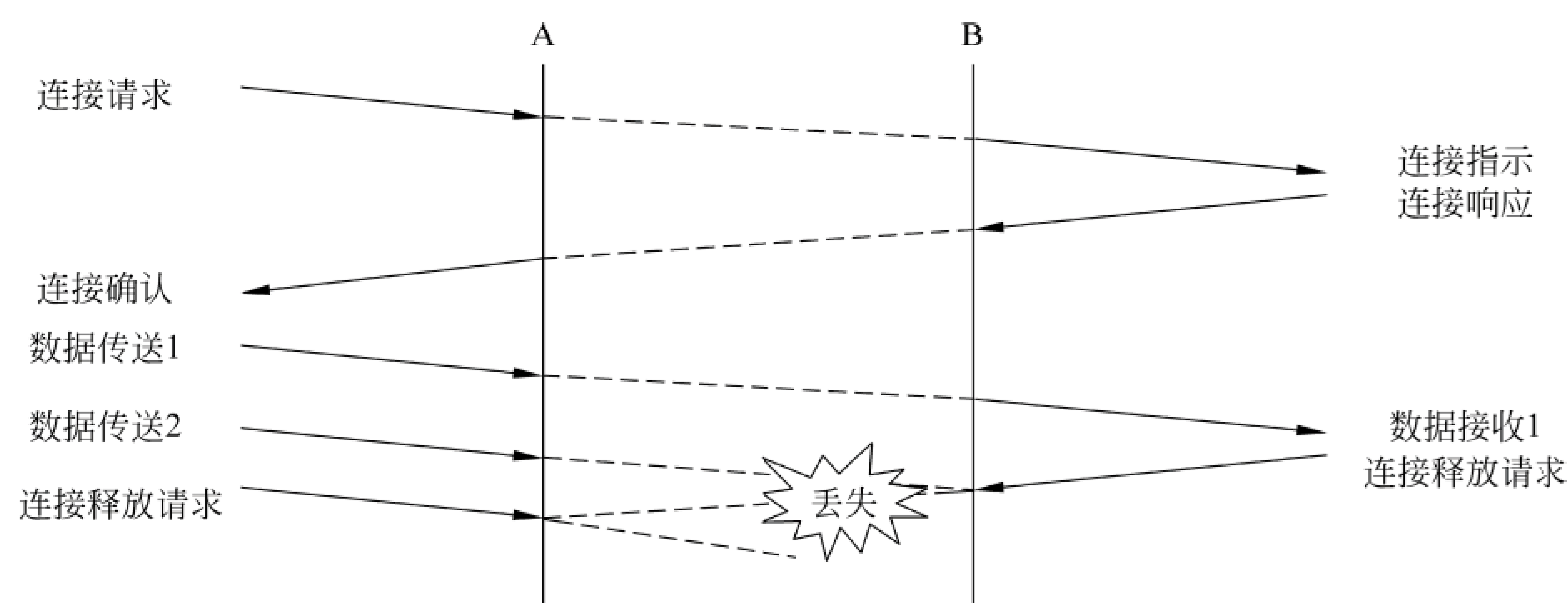


图 3.6　断连不当引起数据丢失

为了防止因断连不当引起的数据丢失，断连应选择在确信对方已经收到自己发送的数据并且自己和对方不再发送数据时。进行由于 TCP 连接是双工的，它包含了两个方向的数据流传送，形成两个“半连接”。在撤销时，一方发起撤销连接但连接依然存在，要在征得对方同意之后，才能执行断连操作。

下面分两种情况考虑连接释放问题：传输正常结束释放和传输非正常结束释放。

1）传输正常结束释放

数据传输正常结束后，就应当立即释放这次 TCP 连接所占用的资源。所以连接的双方都可以发起释放连接。如图 3.7 所示为一个由 A 方先发起的连接可靠释放过程。一般它是一个 4 次握手过程。

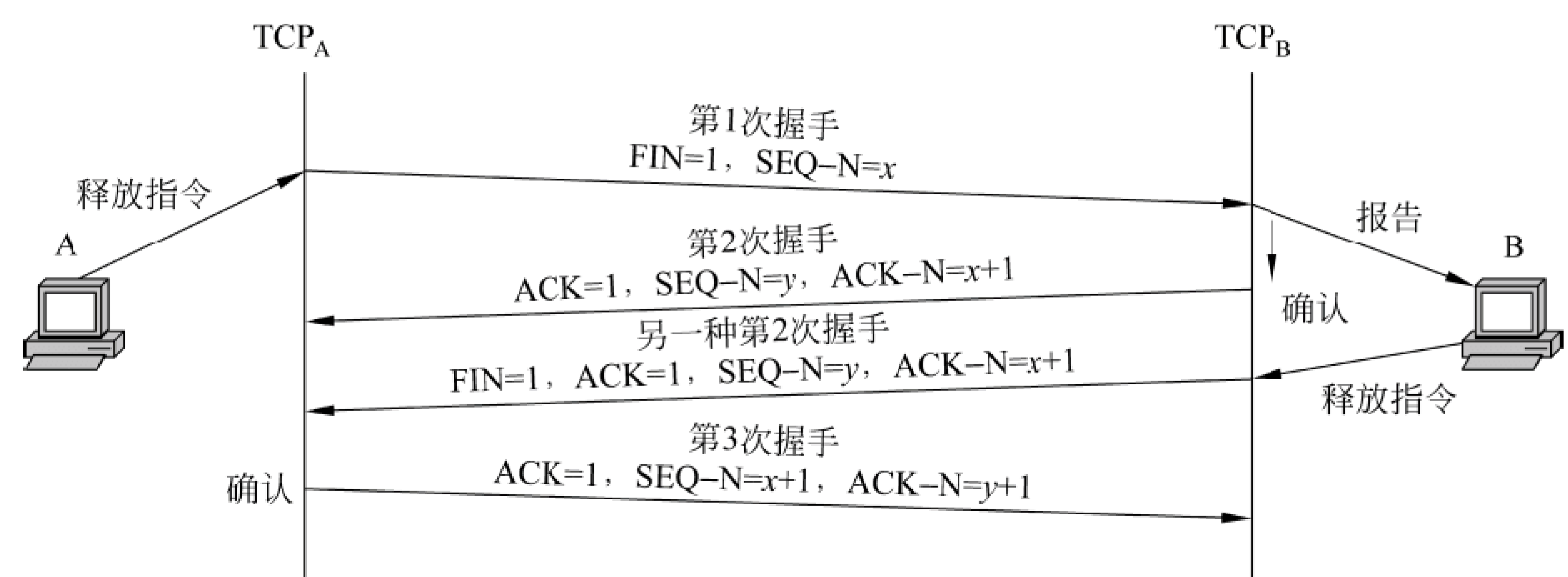


图 3.7　A 方先发起的连接可靠释放过程

第 1 次握手：主机 A 先向 TCP_A 发出连接释放指令 FIN，并不再向传输层发送数据；T_{CPA} 向 T_{CPB} 发送释放通知报文，内容如下。

- FIN=1：A 已经没有数据发送，要求释放从 A 到 B 的连接。
- SEQ–N=x：本次连接的初始序列号（即已经传送过的数据的最后一个字节的序号加 1）为 x。

第 2 次握手：TCP_B 收到 TCP_A 的连接释放通知 FIN 后，向 TCP_A 发确认报文，内容如下。

- ACK=1：确认报文。
- ACK–N = x +1：确认了序号为 x 的报文。
- SEQ–N = y：自己的序号为 y。

这时，从 TCP_A 到 TCP_B 的半连接就被释放。而从 TCP_B 到 TCP_A 的半连接还没有释放，从 TCP_B 还可以向 TCP_A 传送数据，连接处于半关闭（half-close）状态。如果要释放从 TCP_B 到 TCP_A 的连接，还需要进行类似的释放过程。这一过程可以第 1 次握手后开始，即选择另一种第 2 次握手。

另一种第 2 次握手：TCP_B 收到 TCP_A 的连接释放通知后，即向主机 B 中的高层应用进程报告，若主机 B 也没有数据了，主机 B 就向 TCP_B 发出释放连接指令，并携带对于 TCP_A 释放连接通知的确认。报文内容如下。

- FIN=1，ACK=1：释放连接通知报文，携带了确认。
- SEQ–N=y，ACK-N = x+1：确认了序号为 x 的报文，自己的序号为 y。

第 3 次握手：TCP_A 对 TCP_B 的释放报文进行确认。报文内容如下。

- ACK=1：确认报文。
- SEQ–N = x+1，ACK-N = y+1：本报文序列号为 x + 1；确认了 TCP_B 传送来的序号为 y 的报文。

这时，从 TCP_B 到 TCP_A 的连接也被释放。

2）传输非正常结束释放

在有些情况下，希望 TCP 传输立即结束。为了提供这种服务，当一方突然关闭时，TCP 会立即停止发送和接收，清除发送和接收缓冲区，同时向对方发送一个 RST=1 的报文，要求重新建立连接。

3.1.5 TCP 数据传输

1．确认和超时重传机制

TCP 传输的可靠性在于其使用了序号和确认：发送方通知发送序号，接收方在此基础上确认（用期望序号表示）。同时，为了防止发送后接收方收不到的情况，TCP 每发送一个报文，就在自己的重发队列中存放一个该报文的副本，并对此报文设置一个计时器，为超时重发做准备。如果一个 TCP 段在规定的时间片内收不到确认（接收端没有收到报文或报文错误，都不发确认），就重传该报文。

2．流量与拥塞控制

TCP 采用滑动窗口进行流量和拥塞控制。TCP 的流量控制“窗口”是一种可变窗口。当接收方用户没有及时取走滞留在 TCP 缓冲区的数据时，会占用系统资源，窗口将变小；当接收方取走在 TCP 缓冲区中的数据时，释放了系统资源，窗口将变大。也就是说，TCP 允许随时改变窗口大小，这样不仅可以提供可靠传输，还可以提供很好

的流量控制。

与可变窗口相配套的是窗口通告（window advertisement），即每个确认中，除了要指出已经收到的 8 位组序号外，还包括一个窗口通告，用于说明接收方窗口（接收缓冲区）还有多大——能接收多少个 8 位组数据。发送方要以当前记录的接收方最新窗口大小为依据决定发送多少 8 位组。所以通常也把接收端窗口（receiver window，rwnd）称为通告窗口（advertised window）。

3. 拥塞控制的慢开始与拥塞避免算法

TCP 通过通告窗口，使得发送端的发送能力不大于接收端的接收能力。但是，这样并不能完全避免网络拥塞。因为网络是一个多结点的系统，其拥塞状况并不完全取决于某个接收方的接收能力。在这种情况下，为了避免网络拥塞状况恶化，发送端还需要根据网络的拥塞程度调整自己的发送能力。为此，除了要设置一个按照接收方接收能力决定的通告窗口外，还要设置一个按照网络拥塞程度决定的一个发送窗口限制——拥塞窗口（congestion window，简写为 cwnd）。显然，实际的发送窗口的上限应当取通告窗口与拥塞窗口中的小者。

慢开始和拥塞避免算法是早期使用的决定拥塞窗口大小的两个算法。

（1）慢开始算法：首先设置 cwnd 为 1 个 MSS（Maximum Segment Size，最大报文段中的数据字节数），以后每收到其 ACK 后，将 cwnd 增加至多一个 MSS 值，再发送相应数量的报文段。这样，在不出现拥塞的情况下：

第 1 次发送后，cwnd 将增加为 2 个 MSS，即一次具有 2 个 MSS 的发送能力；

第 2 次发送后，cwnd 将增加为 4 个 MSS，即一次具有 4 个 MSS 的发送能力；

……

拥塞窗口呈指数规律增长。

（2）拥塞避免算法不是按照收到的 ACK 数量增加 cwnd，而是按照时间，即每经过一个往返时延 RTT，增加一个 MSS 大小，使 cwnd 呈线性增长。

为了控制拥塞状况，要设置一个门限 ssthesh（通常设置为 65 535 字节，即 16 个报文段），形成如下拥塞控制算法：

（1）比较 cwnd 与 ssthesh。

- cwnd < ssthesh，继续执行慢开始算法；
- cwnd > ssthesh，停止慢开始算法，改用拥塞避免算法；
- cwnd = ssthesh，可执行慢开始算法。也可执行拥塞避免算法。

（2）将发送窗口设置为通告窗口与拥塞窗口中的小者。

（3）网络每出现一次拥塞（出现某个报文段的超时），就执行一次 ssthesh=0.5×ssthesh 的计算（但不能小于 2MSS）。这个计算被称为“乘法减小”（multiplicative decrease）原则。

（4）若执行拥塞避免算法后，发送端能够收到所有发出报文的确认，便要执行 cwnd=cwnd+MSS 的操作。这称为“加法增大”（odditive increase）原则。

按照上述算法，可以得到如图 3.8 所示的 TCP 拥塞窗口变化规律。

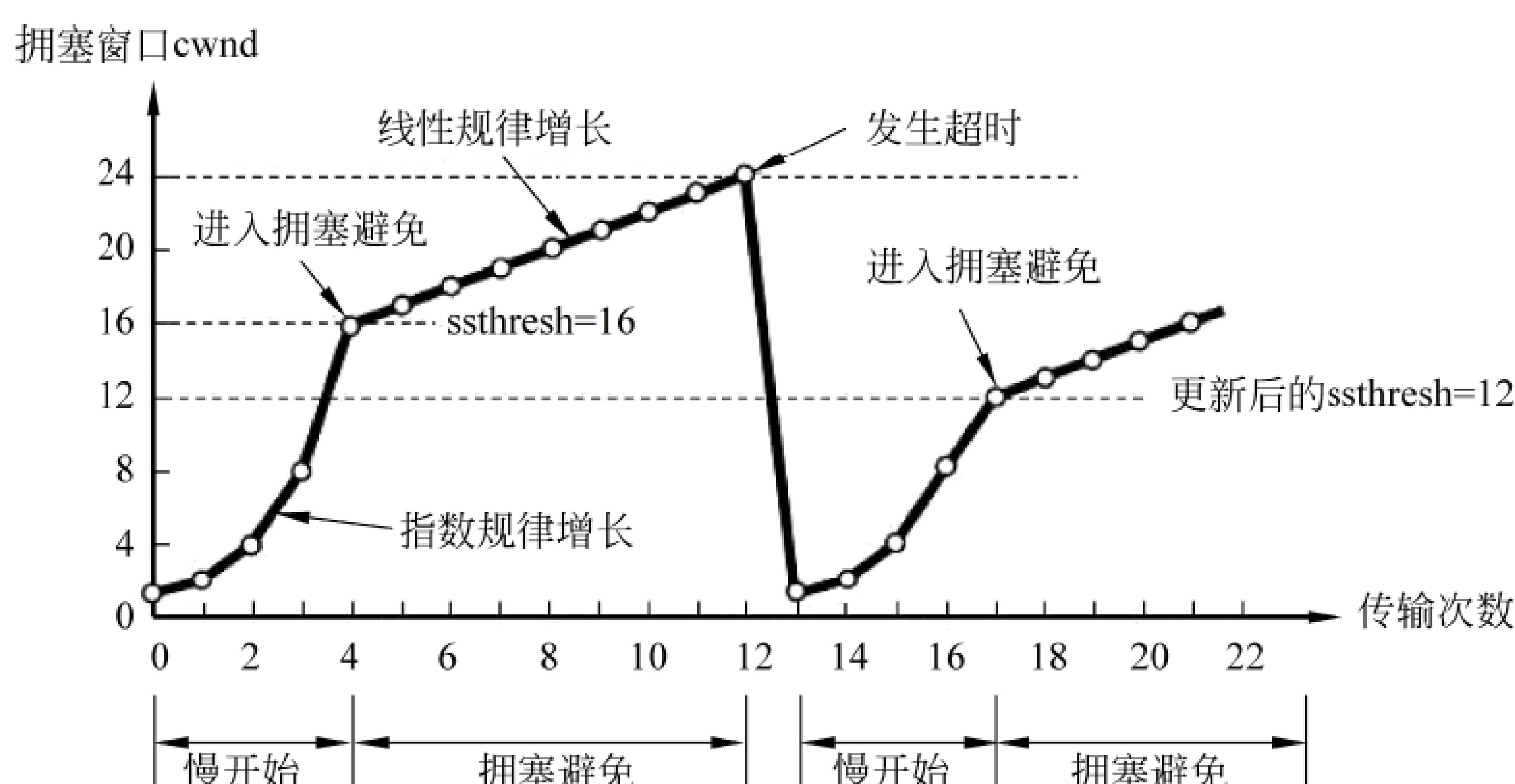


图 3.8　采用慢开始和拥塞避免算法的 TCP 拥塞窗口变化规律

4. 拥塞控制的快重传和快恢复

慢开始和拥塞避免算法在有些情况下会让 TCP 等待某个数据段的超时后才重新开始发送丢失的报文段。例如，发送端连续发送报文段 M_1~M_6。则接收方在收到 M_1 和 M_2 后，将发出 ACK_2 和 ACK_3。若所发送的报文 M_3 丢失，则收到 M_4 后发出的仍然是 ACK_3；收到 M_5 后发出的仍然是 ACK_3，收到 M_6 后发出的仍然是 ACK_3。尽管收到这么多 ACK_3，但是发送段还是要等到 M_3 的重传计时器超时后，才重传 M_3。

快重传的基本思想是早些重传丢失报文段，它规定只要收到某个报文段的 3 个重复的 ACK，就要立即重发该报文段，而不必等待其重传计时器超时。

在尽早开始重传的同时，还可以使用快恢复算法使网络出现拥塞后尽快使网络恢复到正常工作状态。将快重传和快恢复结合起来，形成下面的算法：

（1）当发送端连续收到三个重复的 ACK 时，则按照“乘法减小”的原则，重新设置慢开始门限 ssthresh。

（2）设置拥塞窗口 cwnd 为 ssthresh+ n×MSS。n（≥3）为收到的 ACK 的数量。因为收到的 n 个重复的 ACK，是接收端对已经到达的 3 个报文的应答。这 n 个报文段已经保存在接收端的缓存中。所以网络中不是堆积了报文，而是减少了报文。这比慢开始将拥塞窗口设置为 1，要恢复得快。

（3）若发送窗口还允许发送报文段，就按拥塞避免算法继续发送报文段。

（4）若收到了确认新的报文段的 ACK，就将 cwnd 缩小到 ssthresh。

这是一种可以明显改进 TCP 性能的算法。

5. TCP 的紧急数据传输

用户有时要发送一些紧急的数据，例如在一个要运行很长时间的程序执行过程中取消该程序的运行等，需要发出由 Control+C 两个字符组成的中断命令。这时，就需要将紧急发送的报文段中的 URG 位置 1，以告诉 TCP 这个报文段中有紧急数据，同时将这两个字符插入到报文段的数据字段的前面，并用一个紧急指针（Urgent Pointer）指出紧急数据的最后一个字节的序号，以通知接收方紧急数据的大小。接收方即使窗口为 0，发送方也可以发送紧

急数据。

接收方收到紧急数据并处理完后，TCP 即通知应用程序恢复到正常工作。

3.1.6 UDP

UDP 是一个无连接的协议，在发送时无须建立连接，仅仅向应用程序提供了一种发送封装的原始 IP 数据报的方法。如图 3.9 所示为 UDP 数据报格式。其中校验和是可选的，当不进行校验时，这个域为 0。

UDP源端口	UDP目的端口
UDP数据报长度	UDP校验和
UDP数据区	

图 3.9 UDP 数据报格式

UDP 是一个基于不可靠通信子网的不可靠传输层协议。因此，基于 UDP 的应用程序必须自己解决可靠性问题，如报文丢失、报文重复、报文失序、流量控制等。

应用程序可以使用 UDP 进行通信。不同的进程用不同的端口号进行标识。端口号分为公认（众所周知）端口号和自由端口号两种。

在 UNIX 系统中，一个 UDP 端口是一个可读和可写的软件结构，UDP 为每个端口维护一个接收缓冲区。发送数据时，UDP 将数据内容生成一个 UDP 数据报，然后交给网络层的 IP 发送。接收数据时，UDP 从网络层 IP 接收到 UDP，然后根据目的端口号将其放在相应的接收缓冲区中。如果没有匹配的端口号，UDP 将丢弃该数据报，并向发送主机返回一个“不可到达”的 ICMP 消息；如果匹配端口号已满，UDP 也丢弃该数据报，但不回送错误消息，该数据报要靠超时重发。

UDP 的优点在于高效率，通常用于交易型应用，一次交易只有一来一往两次报文交换。

3.2 IPv4

IP 层是基于网络互联的 TCP/IP 计算机网络体系中关键的一层。在传输层虽然解决了进程之间的通信问题。但由于进程是运行在主机上的，因此只有解决了主机之间的通信问题，才能有进程之间的通信。因此需要解决如下 3 个关键问题。

（1）主机运行在不同网络之中，为此需要解决对于源主机和目标主机的识别问题。因此 IP 提出了一套对于网络和主机的编号规则——IP 地址协议。

（2）主机到主机需要经过一系列的网络，为此需要解决数据的传输路径问题，因此提出了一套路径选择的算法——路由协议。

（3）在传输层，报文分段是根据端主机之间的接收能力进行分段的。这些分段在 IP 层，则要按照网络之间的路由能力进一步切分封装成分组传输。

目前广为应用的 IP 是其第 4 个版本——IPv4。

3.2.1 IP 分组格式

1. IP 分组的形成

在 IP 层要对传输层的数据进行分片，并进一步加上 IP 头，封装 IP 分组。如图 3.10 所示，每个分组都是一个两层封装：外封装是 IP 头，内封装的从传输层传来的 TCP 或 UDP 头。

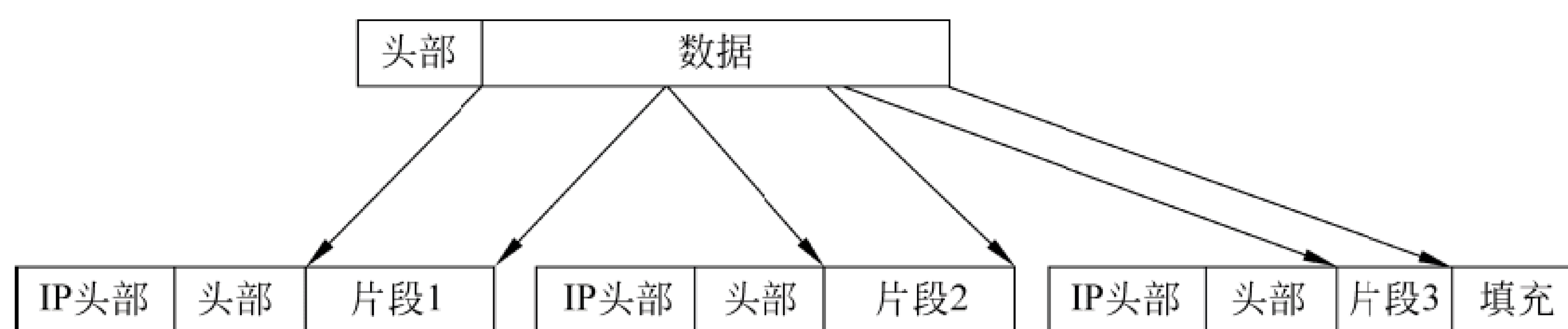


图 3.10　IP 数据分组的形成

在 IP 分组中，对于数据部分规定了一定的长度。最后一个分组中的数据是前面分片剩余的数据，长度往往不正好是规定的长度，不足部分需要进行填充。

2. IPv4 分组格式

图 3.11 为 IPv4 分组格式。

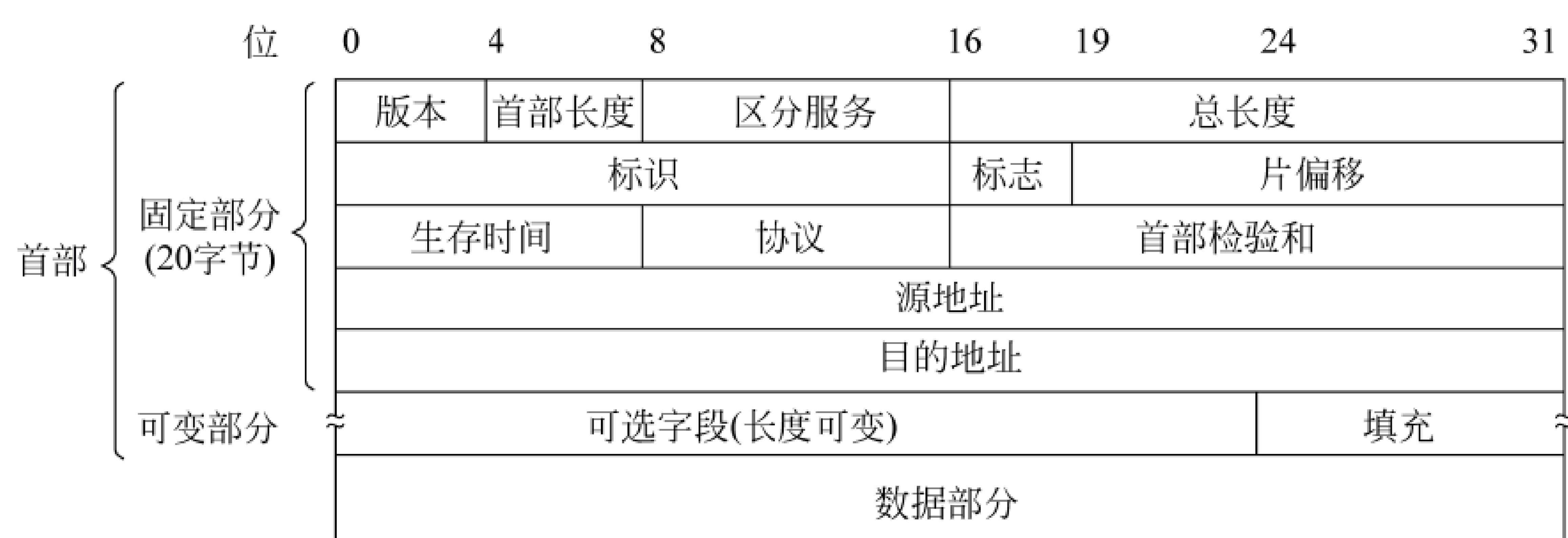


图 3.11　IPv4 分组格式

下面介绍 IPv4 分组首部各字段的意义。

1）IPv4 分组首部的固定部分各字段含义

（1）版本。占 4b，指 IP 协议的版本。通信双方使用的 IP 协议版本必须一致。目前广泛使用的 IP 协议版本号为 4（即 IPv4）。关于 IPv6，目前还处于试用阶段。

（2）首部长度。占 4b，可表示的最大十进制数值是 15。请注意，这个字段所表示数的单位是 32 位（4B）字长，因此，当 IP 的首部长度为 1111 时（即十进制的 15），首部长度就达到 60B。若 IP 分组的首部长度不是 4B 的整数倍时，就必须利用最后的填充字段加以填充。因此数据部分永远在 4 字节的整数倍开始，以便于实现 IP 协议。首部长度限制为 60B 的缺点是有时可能不够用，但能使用户尽量减少开销。最常用的首部长度就是 20B（即首部长度为 0101），这时不使用任何选项。

（3）区分服务。占 8b，用来获得更好的服务。这个字段在旧标准中叫作服务类型，被分为 3 个部分：

- 优先级子字段（3b），即前 3b，用 0～7 表示优先级别高低。但现在已经不用。
- 第 8 位保留未用。
- TOS，中间 4b，分别代表：最小时延、最大吞吐量、最高可靠性和最小费用。每种服务类型中只能置其中 1 比特为 1。可以全为 0，若全为 0 则表示一般服务。

表 3.2 列出了对不同应用建议的 TOS 值。例如，TELNET 协议可能要求有最小的延迟，FTP 协议（数据）可能要求有最大吞吐量，SNMP 协议可能要求有最高可靠性，NNTP（Network News Transfer Protocol，网络新闻传输协议）可能要求最小费用，而 ICMP 协议可能无非凡

要求（4 比特全为 0）。实际上，大部分主机会忽略这个字段，但一些动态路由协议如 OSPF（Open Shortest Path First Protocol）、IS-IS（Intermediate System to Intermediate System Protocol）可以根据这些字段的值进行路由决策。

表 3.2　对不同应用建议的 TOS 值

应用程序	最小时延	最大吞吐量	最高可靠性	最小费用	十六进制值
Telnet/Rlogin	1	0	0	0	0x10
FTP					
控制	1	0	0	0	0x10
数据	0	1	0	0	0x08
任意块数据	0	1	0	0	0x08
TFTP	1	0	0	0	0x10
SMTP					
命令阶段	1	0	0	0	0x10
数据阶段	0	1	0	0	0x08
DNS					
UDP 查询	1	0	0	0	0x10
TCP 查询	0	0	0	0	0x00
区域传输	0	1	0	0	0x08
ICMP					
差错	0	0	0	0	0x00
查询	0	0	0	0	0x00
任何 IGP	0	0	1	0	0x04
SNMP	0	0	1	0	0x04
BOOTP	0	0	0	0	0x00
NNTP	0	0	0	1	0x02

（4）总长度。总长度指首部和数据之和的长度，单位为字节。总长度字段为 16b，因此分组的最大长度为 $2^{16}-1=65\ 535$B。

在 IP 层下面的每一种数据链路层都有自己的帧格式，其中包括帧格式中的数据字段的最大长度，这称为最大传送单元 MTU（Maximum Transfer Unit）。当一个分组封装成链路层的帧时，此分组的总长度（即首部加上数据部分）一定不能超过下面的数据链路层的 MTU 值。

（5）标识（identification）。占 16b。IP 软件在存储器中维持一个计数器，每产生一个分组，计数器就加 1，并将此值赋给标识字段。但这个“标识”并不是序号，因为 IP 是无连接服务，分组不存在按序接收的问题。当分组由于长度超过网络的 MTU 而必须分片时，这个标识字段的值就被复制到所有分组的标识字段中。相同的标识字段的值使分片后的各分组片最后能正确地重装成为原来的分组。

（6）标志（flag）。占 3b，但目前只有 2b 有意义。

- 标志字段中的最低位记为 MF（More Fragment）。MF=1 表示后面“还有分片”的

分组。MF=0 表示这已是若干分组片中的最后一个。

- 标志字段中间的一位记为 DF（Don't Fragment），意思是“不能分片”。只有当 DF=0 时才允许分片。

（7）片偏移。占 13b。片偏移指出：较长的分组在分片后，某片在原分组中的相对位置。也就是说，相对用户数据字段的起点，该片从何处开始。片偏移以 8B 为偏移单位。这就是说，每个分片的长度一定是 8B（64b）的整数倍。

（8）生存时间。占 8b，常用的 TTL（Time To Live）表示，由发送数据的源主机设置，限制分组最多可以经过的路由器数。通常为 32、64、128 等。每经过一个路由器，其值减 1，直到 0 时该数据报被丢弃。防止分组进入死循环。

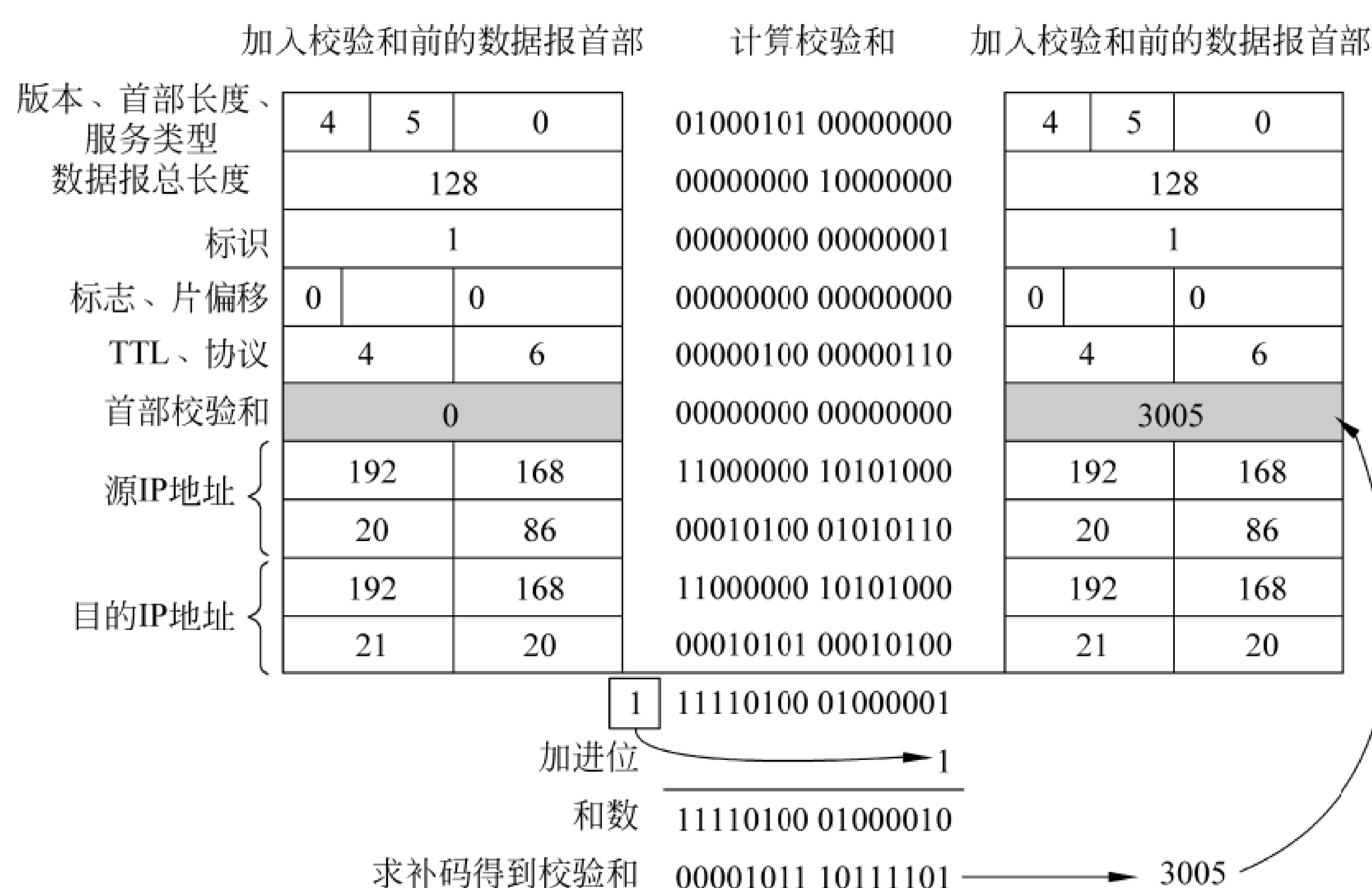
（9）协议。占 8b，协议字段指出此分组携带的数据是使用何种协议，以便使目的主机的 IP 层知道应将数据部分上交给哪个处理过程。表 3.3 为常用协议的协议字段值。

表 3.3　常用协议的协议字段值

协议名	ICMP	IGMP	特殊 IP	TCP	EGP	IGP	UDP	IPv6	ESP	OSPE
协议字段值	1	2	4	6	8	9	17	41	50	89

表中的“特殊 IP”指被封装到 IP 分组中的 IP 分组。

（10）首部检验和。占 16b。这个字段只检验分组的首部，不包括数据部分。这是因为分组每经过一个路由器，路由器都要重新计算一下首部检验和（一些字段，如生存时间、标志、片偏移等都可能发生变化）。不检验数据部分可减少计算的工作量。为了使读者对于首部校验和有进一步了解，图 3.12（a）给出了发送端计算校验和的过程，图 3.10（b）给出了接收端检验校验和的过程。



(a) 发送端计算校验和

图 3.12　IP 分组中的校验和使用实例

		计算校验和
版本、首部长度、服务类型	4 | 5 | 0	01000101 00000000
数据报总长度	128	00000000 10000000
标识	1	00000000 00000001
标志、片偏移	0 | | 0	00000000 00000000
TTL、协议	4 | 6	00000100 00000110
首部校验和	3005	00001011 10111101
源IP地址	192 | 168	11000000 10101000
	20 | 86	00010100 01010110
目的IP地址	192 | 168	11000000 10101000
	21 | 20	00010101 00010100
		11111111 11111110
加进位		1
和数		11111111 11111111
求补码得到校验和		00000000 00000000

(b) 接收端检验校验和

图 3.12（续）

（11）源 IP 地址、目标 IP 地址字段：各占 32b，用来标明发送 IP 数据报文的源主机地址和接收 IP 报文的目标主机地址。

2）IP 分组首部的可变部分

IP 首部的可变部分就是一个可选字段。选项字段用来支持排错、测试以及安全等措施，内容很丰富。此字段的长度可变，从 1 个字节到 40 个字节不等，取决于所选择的项目。某些选项项目只需要 1 个字节，它只包括 1 个字节的选项代码。但还有些选项需要多个字节，这些选项一个个拼接起来，中间不需要有分隔符，最后用全 0 的填充字段补齐成为 4 字节的整数倍。

增加首部的可变部分是为了增加 IP 分组的功能，但这同时也使得 IP 分组的首部长度成为可变的。这就增加了每一个路由器处理分组的开销。实际上这些选项很少被使用。新的 IP 版本 IPv6 就将 IP 分组的首部长度做成固定的。

目前，这些任选项定义如下：

（1）安全和处理限制（用于军事领域）。

（2）记录路径（让每个路由器都记下它的 IP 地址）。

（3）时间戳（让每个路由器都记下它的 IP 地址和时间）。

（4）宽松的源站路由（为分组指定一系列必须经过的 IP 地址）。

（5）严格的源站路由（与宽松的源站路由类似，但是要求只能经过指定的这些地址，不能经过其他的地址）。

这些选项很少被使用，并非所有主机和路由器都支持这些选项。

3.2.2 IP 地址格式

1. IP 地址分类

TCP/IP 是面向网络互连而建立的一种网络体系。为了进行网络互联，就要考虑不同的

网络互联之后，一个网络中的某台主机与另一个网络中的某台主机之间的通信问题。也就需要对所有连接起来的主机进行编码。为此提出了一套编码标准，这个编码标准称为 IP 地址。所有想要连接在 Internet 中的网络或计算机必须遵循这个规则，申请到合法的 IP 地址，才可以被识别，进行通信。

IPv4 规定的 IP 地址是 32b 编码，即 4B。为了便于理解和记忆，通常将每个字节用一个十进制数表示，并用小数点分隔，称为点分十进制（dotted decimal notation）码。例如某 IP 地址为

10000000 00001010 00000010 00011110

可以写为

128.10.2.30

如图 3.13 所示，IP 地址可分为三部分：

- 类型标志，分为 A、B、C、D、E 五类，分别用 0、10、110、1110 和 11110 标识。
- 网络标识符（netID）。
- 主机编号（hostID）。

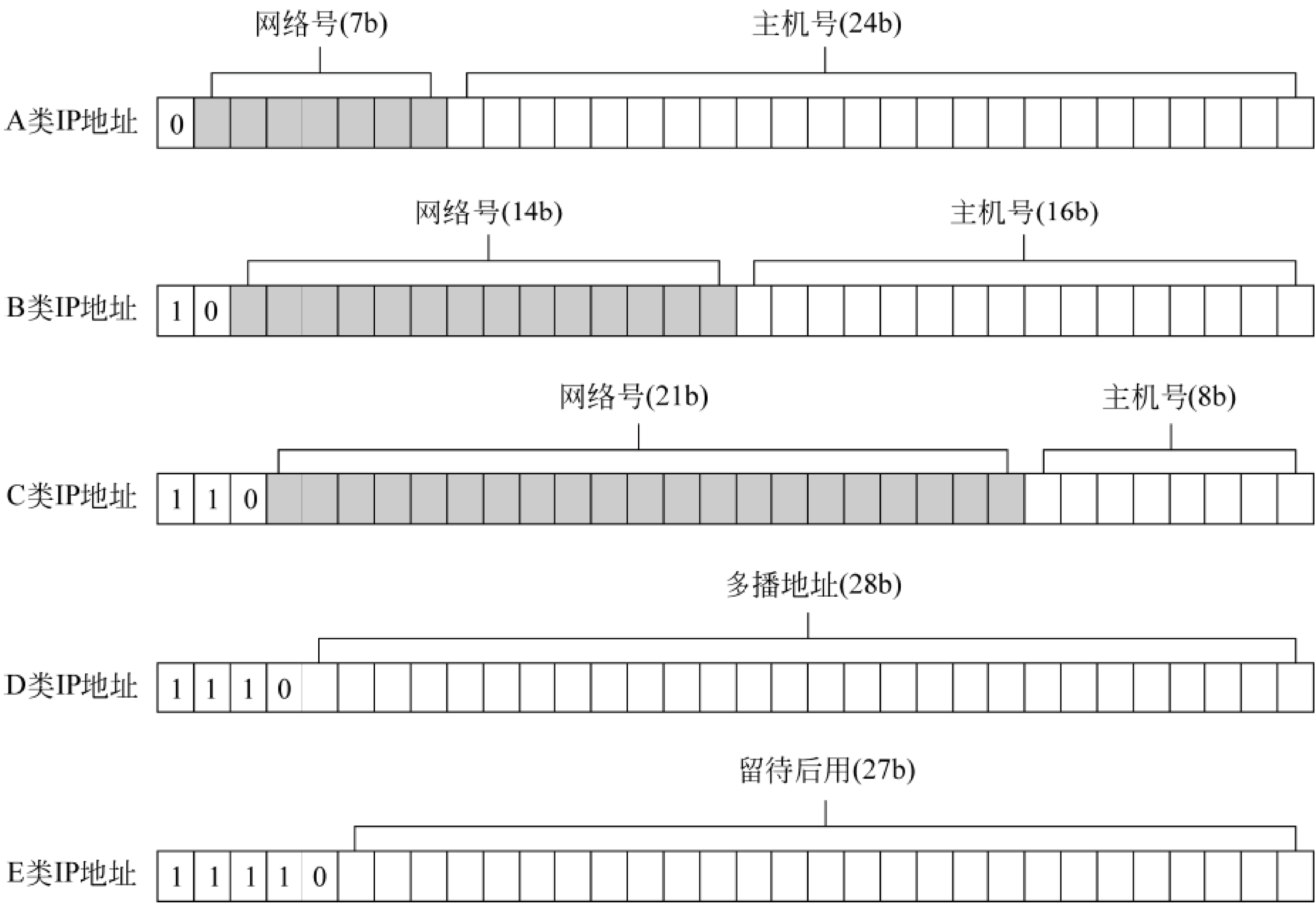


图 3.13　五类 IPv4 地址结构

A、B、C 是 3 类基本地址类型，区别仅在于网络大小不同，如表 3.4 所示。

表 3.4　A、B、C 三类基本 IP 地址类型与规模

类别	类型标识	网络规模	netID 位数	可编址网络数	hostID 位数	每个网络最多主机数	IP 地址范围
A	0	巨型网络	7	126	24	16777214	1.0.0.0～127.255.255.255
B	10	大型网络	14	16383	16	65534	128.0.0.0～191.255.255.255
C	110	中小型网络	21	2097151	8	254	192.0.0.0～255.255.255.255

D 类地址是一种多址广播地址格式，用 1110 作为标志，netID 的范围为 224～239。

E 类地址是为研究和实验保留的地址，用 11110 作为标志，netID 的范围为 240 及以上。例如，上述 128.10.2.30，显然是一个 B 类地址。由于 B 类地址网络地址占 2B，所以，其网络地址为 128.10，网络内主机地址为 2.30。

2. IP 地址的重要特点

（1）在 Internet 网络中，只用 IP 地址中的 netID 来标识主机所在的网络，即 netID 相同的主机就认定是网络中的主机，不管它们物理上是如何连接的。

（2）不同 netID 的局域网或主机之间必须使用路由器连接。

（3）路由器一个端口用来连接一个网络。当一台路由器连接多个网络时，它的多个端口都会有一个 netID 不同的 IP 地址。一台路由器最少连接两个网络，即它最少有两个 netID 不同的 IP 地址。

（4）路由器仅根据 netID 转发分组，即路由表中只需存储网络号，无须存储主机号。这样可以减少路由表的存储量，提高路由器的处理速度。

（5）两台路由器可以直接相连。这时，在这条连线就被看成一个逻辑上的网络，其连接的两个端口可以分配一个 IP 地址，也可以不分配。若不分配 IP 地址，就被称为无编号网络（unnumbered network）或匿名网络（anonymous network）。

（6）一台主机也可以拥有两个 netID 不同的 IP 地址。这样的主机称为多属主机（multihomed host）。

3. IP 地址的使用约束

1）私有 IP 地址

在规划的时候，将 IP 地址分为私有地址和公有地址，私有地址只能在内部网络使用，不能在互联网使用，认为这样的地址是互联网的不合法地址。在 A、B、C 三类地址中都选择一部分地址作为私有地址：

A 类地址中，netID 为 10 的所有 IP 地址。

B 类地址中，netID 为 172.16~172.31 的所有 IP 地址。

C 类地址中，netID 为 192.168 的所有 IP 地址。

2）受限 IP 地址

netID 全 0，只用作源地址，表示本网，不路由；若 hostID 全 0，在 DHCP 协议中指本机。

netID 为 1（全 255），仅用作目的地址，代表所有网络；若若 hostID 全 0，仅作子网掩码。

hostID 全 0，仅表示网络地址，不可用作源地址。

hostID 全 1，不可作源地址，仅向指定网络广播。

netID 为 127，仅可以用作本地软件环回测试。

4. IP 地址的分配与申请

为了确保一个 IP 地址对应一台主机，IP 地址由 IANA（Internet Assigned Numbers Authonty，互联网名称与数字地址分配机构）统一编号，并交由 Internet 名字与号码指派公

司 ICANN（Internet Corporation for Assigned Names and Numbers）进行统一分配。ICANN 将地址的分配授权给 RIR（Regional Internet Registry，区域性互联网注册机构）负责地区的登记注册申请。现在全球有 5 个 RIR：

（1）RIPE（Reseaux IP Europeans）欧洲 IP 地址注册中心——服务于欧洲、中东地区和中亚地区；

（2）LACNIC（Lation American and Caribbean Internet Address Registry）拉丁美洲和加勒比海 Internet 地址注册中心——服务于中美、南美以及加勒比海地区；

（3）ARIN（American Registry for Internet Numvers）美国 Internet 编号注册中心——服务于北美地区和部分加勒比海地区；

（4）AFRINIC（Africa Network Information Centre）非洲网络信息中心——服务于非洲地区；

（5）APNIC（Asia Pacific Network Information Centre）亚太地址网络信息中心——服务于亚洲和太平洋地区的国家。

另外，许多国家和地区都成立了自己的域名系统管理机构，负责从前述 3 个机构获取 IP 地址资源后在本国或本地区的分配与管理事务。这些国家和地区的域名系统管理机构大多属于半官方或准官方机构。但在实际运作过程中，相关国家或地区的政府至少在业务上对其不加干预，使其成为前述 3 个机构之一在各该国家或地区的附属机构。如日本的 JPNIC 和中国的 CNNIC 均属此种机构。

获得公有 IP 地址的方法：向 InterNIC 申请，也可以向 ISP 申请。

3.2.3　子网划分与子网掩码

1. 子网与子网编码

任何一个 A、B、C 类 IP 地址都对应着一定规模（主机数目）的网络，是一种二级地址。当实际的网络规模接近 IP 地址的主机 ID 上限时，该 IP 地址才能得到充分利用。例如，一个实际网络中的主机数为 250 台左右时，申请一个 C 类地址最为合理。若实际的网络规模较小，如只有 30 台左右的主机时，独自占用一个 C 类地址会造成地址资源的浪费，较合理的做法是将一个 C 类地址分给若干个小的网络共同使用。具体办法是从 hostID 域中借用某几位高位作为子网的 subnetID 域，形成如图 3.14 所示的三级地址。

这样，网关（连接物理网络的路由器）的路由表就被分成两级：先识别由 NetID 标识的路由，以确定一个逻辑的网络；再在该逻辑的网络内部用 SubnetID 来确定具体的子网。

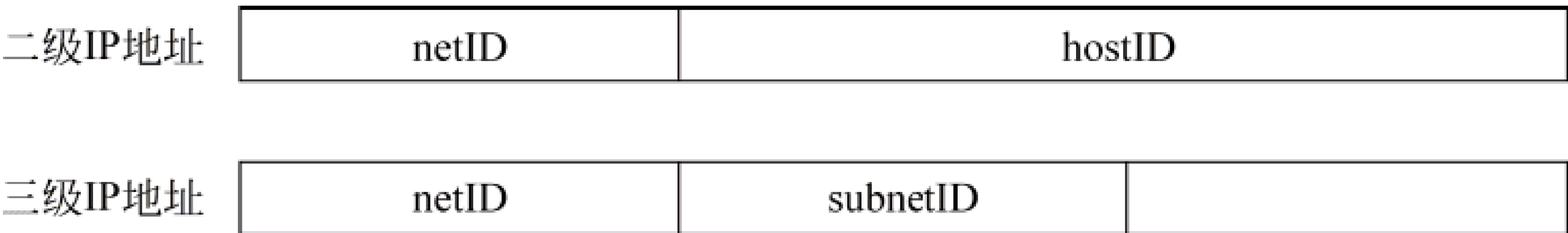


图 3.14　三级 IP 地址结构

2. 子网掩码与子网划分

三级 IP 地址提供了有效的、灵活的使用 IP 地址资源的手段。但是，带来的问题是：路由器如何判断到底一个 IP 地址中有多少位用于子网编码呢？在二级地址中，可以用类型标

识来判断这个 IP 地址是哪类地址，得到 netID 有多少位的信息。在三级 IP 地址中，虽然还有这个信息，但没有 subnetID 是多少位的信息了。为此必须另外提供一个关于网络码有多少位的信息，这个信息用子网掩码（sunnet mask）表示。

子网掩码是一种 32 位的位模式。RFC 文档中规定：每个使用子网的结点都选择一个 32 位的位模式，用这个位模式的 1 位来对应 IP 地址中网络地址（包括 netID 和 subnetID）中的一位，用位模式中的 0 位来对应 IP 地址中主机地址中的一位。虽然，RFC 文档中没有强求子网掩码中的 1 和 0 必须连续，但这种连续的 1 和 0，可以清晰地表明哪一段是网络地址，哪一段是主机地址。

子网掩码的作用是进行子网划分。划分的方法是对 IP 地址与子网掩码进行“与”运算，得到的就是子网的网络地址。图 3.15 为一个子网划分的实例。

	十进制				
IP地址：	141.14.2.21	10001101	00001110	00000010	00010101
子网掩码：	255.255.255.0	11111111	11111111	11111111	00000000
网络地址：	141.14.2.0	10001101	00001110	00000010	00000000

图 3.15　子网划分实例

例 3.1　将一个有 256 台主机、网络号为 200.15.192 的 C 类型网络分为两个相同的各拥有 128 台主机的子网。

在网络号为 200.15.192 的 C 类网络中，主机的编号为 200.15.211.0～200.15.211.256。由于要将一个 C 类网络分为两个子网，因而要在其 HostID 域中借用最高一位，子网掩码由 C 类的默认掩码 255.255.255.0 变为 255.255.255.128，即

11111111.11111111.11111111.10000000

以此类推，要划分为 4 个子网，应借用 2 位；要划分为 8 个子网，应借用 3 位……

例 3.2　对于一个 C 类网络 202.113.240，可以使用子网掩码 255.255.255.224 划分为 8 个子网，每个子网有 32 个 IP 地址：

202.113.240.0 ～202.113.240.31

202.113.240.32～202.113.240.63

⋮

202.113.240.224～202.113.240.255

应当注意，不管如何划分，一个网络中可容纳的主机总数不会增多。

RFC 950 成为 Internet 的正式标准后，子网掩码随之成为网络或子网的重要信息，所有的网络配置必须确定子网掩码，路由器在与相邻路由器交换路由信息时，必须同时传递子网掩码，即一个路由器连接几个网络，就有几个 IP 地址和相应的子网掩码。

3. 默认子网掩码

路由器要求子网掩码，因此当网络中没有子网时，A、B、C 三类网络就要使用如下默认子网掩码：

- A 类网络：11111111 00000000 00000000 00000000，即 255.0.0.0。
- B 类网络：11111111 11111111 00000000 00000000，即 255.255.0.0。
- C 类网络：11111111 11111111 11111111 00000000，即 255.255.255.0。

3.2.4 无分类编址方法 CIDR 与超网

IP 的无分类编址，也称无分类域间路由选择（Classless Inter-Domain Routing，CIDR），它有如下 3 个特点：

（1）使用变长的“网络前缀”（network-prefix）代替分类地址中的网络号和子网号，形成<网络前缀>+<主机号>的两层 IP 地址结构。其中，网络前缀的位数可以由网络管理员自行定义。与三层的编址相比，CIDR 可以更有效地利用 IPv4 的地址空间。

常用的 CIDR 编址是采用斜线记法（slash notetion），即在地址后面加斜线标以网络前缀占用的位数。如 127.16.34.20/22，表示上述地址中，前 22 位（二进制）用于表示网络前缀，后 10 位表示主机地址。

斜线记法还允许省略低位连续的 0，如 127.0.0.0/22，可以写为 127/22。

（2）CIDR 将网络前缀相同的连续 IP 地址称为“CIDR 地址块”。CIDR 地址块用地址块的起始地址和地址块中的地址数定义，并且也可以用斜线记法表示。例如，127.20.32.0/20 表示该地址块的起始地址为 130.20.32.0，共有 2^{12} 个地址。如图 3.16 所示为其二进制表示。

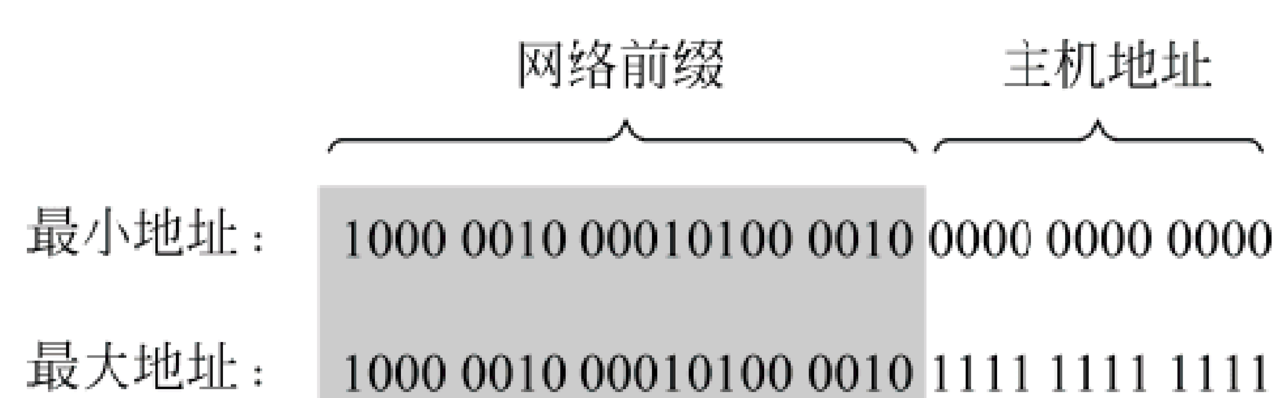


图 3.16　127.20.32.0/20 的二进制表示

这个 CIDR 地址块中的最小地址中的主机地址为全 0，最大地址为全 1。这两个地址一般不用，真正使用的是这两个地址之间的地址。

斜线记法既可以标记单地址，也可以标记块地址。两者的区分要通过上下文分析。

使用 CIDR，不仅可以划分出比 C 类网小的 CIDR 地址块，还可以聚合形成比 C 类地址大的 CIDR 地址块。这样，在路由表中，使用一个网络前缀项目就可以表示多个原来分类地址的路由，形成路由聚合（route aggegation）或构成超网（supernetting）。

（3）路由聚合可以大大减少路由表中的项目数，减少路由器之间的路由选择信息的交换，提高整个 Internet 网络的性能。使用 CIDR 后，路由表的栏目改为由网络前缀和下一跳地址组成。

CIDR 的 RFC 文档(RFC 1517～RFC 1520)于 1993 年形成，现在 CIDR 已经成为 Internet 的建议标准协议。

3.2.5 ICMP 协议

1. ICMP 及其提供的服务

IP 虽然实现了各种不同网络的互联，但由于它提供的是一种不可靠的无连接分组服务，

它关注的重点是如何将数据传输到目的地，至于传输过程中是否有丢失数据包、数据包是否被篡改、IP 分组的顺序是否正确、超时等问题，IP 是无能为力的。然而这些问题又必须处理。为此在 IP 层引入了一个子协议：网际控制消息协议（Internet Control Message Protocol，ICMP）。

ICMP 是一种差错报告机制，它为路由器或目标主机提供了一种方法，使它们能把遇到的差错报告给源主机。

具体地说，ICMP 提供如下服务：

- 测试目的主机可到达性和状态，如接收设备接收 IP 分组时缓冲区是否够用；
- 将不可到达的目的主机报告给源主机；
- 进行 IP 分组流量控制；
- 向路由器发送路由改变请求；
- 检测循环（由此会引发“广播风暴”）或超长路由；
- 报告错误 IP 分组头；
- 获取网络地址；
- 获取子网掩码。

2. ICMP 报文

如图 3.17 所示，ICMP 报文被封装在 IP 分组中，具体内容与类型有关。

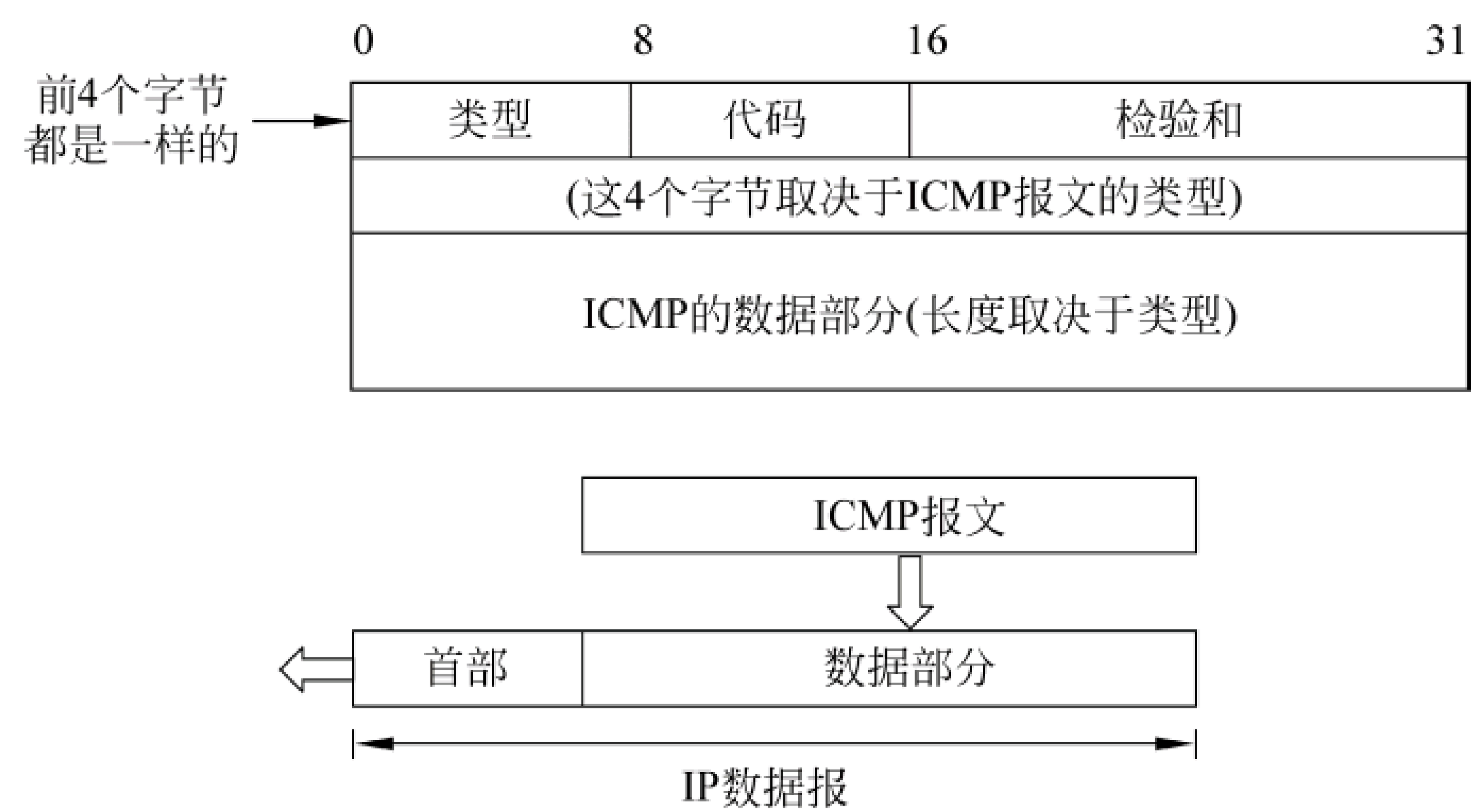


图 3.17　ICMP 报文封装格式

如表 3.5 所示，ICMP 报文分为查询报文和差错报告两大类。每一大类又分为若干种。但常用的有如下几种。

1）*差错报告报文*

发现问题时即刻发送差错报告。报告内容为一个类型数字代码，常用的有 5 种：

- 3，终点不可达，即不能向路由器或主机交付 IP 分组。
- 4，源点抑制（source quench），因拥塞主机或路由器丢弃分组。
- 11，超时，路由器收到 TTL 为 0 的分组。
- 12，参数问题，路由器或主机收到的分组首部中有的字段值不正确。
- 5，改变路由——重定向。

表 3.5　ICMP 报文种类一览表

类型	代码	描　　述	查询	差错	类型	代码	描　　述	查询	差错
0	0	回显应答（Ping 应答）	●		5		重定向：		●
3		目的不可达：				0	对网络重定向		●
	0	网络不可达		●		1	对主机重定向		●
	1	主机不可达		●		2	对服务类型和网络重定向		●
	2	协议不可达		●		3	对服务类型和主机重定向		●
	3	端口不可达		●	8	0	请求回显（Ping 请求）	●	
	4	需要进行分片但设置了不分片比特		●	9	0	路由器通告	●	
	5	源站选路失败		●	10	0	路由器请求	●	
	6	目的网络不认识		●	11		超时：		
	7	目的主机不认识		●		0	传输期间生存时间为 0（Traceroute）		●
	8	源主机被隔离（作废不用）		●		1	在数据报组装期间生存时间为 0		●
	9	目的网络被强制禁止		●	12		参数问题：		
	10	目的主机被强制禁止		●		0	坏的 IP 首部（包括各种差错）		●
	11	由于服务类型 TOS，网络不可达		●		1	缺少必需的选项		●
	12	由于服务类型 TOS，主机不可达		●	13	0	时间戳请求	●	
	13	由于过滤，通信被强制禁止		●	14	0	时间戳应答	●	
	14	主机越权		●	15	0	信息请求（作废不用）	●	
	15	优先权中止生效		●	16	0	信息应答（作废不用）	●	
4	0	源端被关闭（基本流控制）		●	17	0	地址掩码请求	●	
					18	0	地址掩码应答	●	

图 3.18 为差错报告报文的数据字段结构。

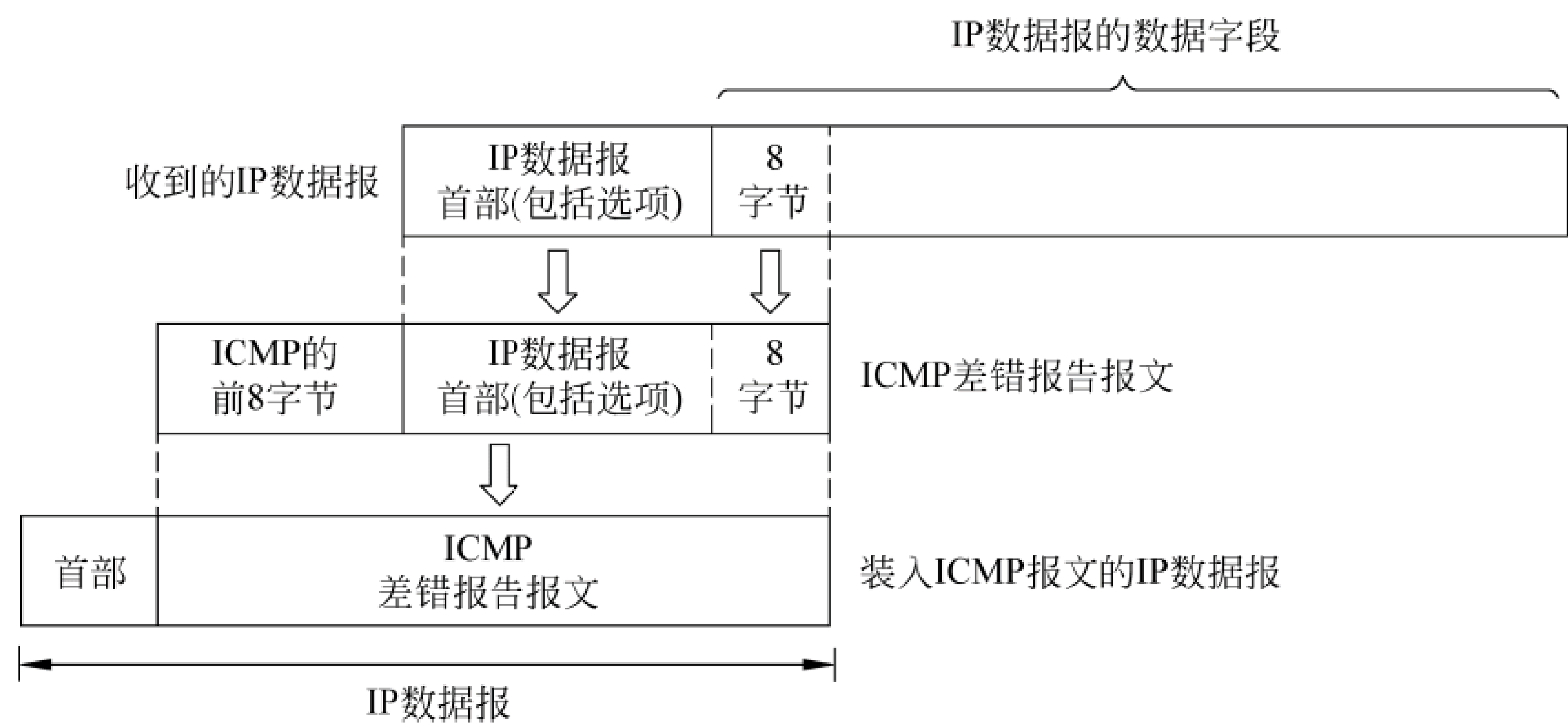


图 3.18　ICMP 差错报告报文的数据字段结构

2）问题不报告报文

下面是遇到问题不发送 ICMP 差错报告报文段情况：

- 对 ICMP 差错报告报文出错。
- 第一份片的分组片的所有后续分组片。

- 具有多播的分组。
- 具有特殊地址（如 127.0.0.0 或 0.0.0.0）的分组。

3）询问报文

发出询问请求和回答询问请求的报文。常用的有两种：

- 8 或 0，回送（echo）请求或回答，一般用来测试目的站是否可以到达等信息。
- 13 或 14，时间戳（timestamp），一般用于测试时钟同步和时间。

3．ICMP 应用举例

ICMP 作为 IP 的补充，使一个路由器或一台目的主机可以通知源主机有关数据分组处理中的错误，并进行必要的处理。下面介绍其两种简单而广泛的应用。

1）ping

ping 是 TCP/IP 网络中一个最简单而又非常有用的 ICMP 应用程序。它使用 ICMP 回应请求/应答，测试一台主机的可达性，验证一个 IP 安装是否正确，具体可以用于下列场合：

- 验证基础 TCP/IP 软件的操作；
- 验证 DNS 服务器的操作；
- 验证一个网络或网络中的设备是否可以被访问。

ping 在不同的实现中语法格式有所不同。下面是在 UNIX 中的应用格式：

```
ping [-switches] host
```

- host：目的主机的名字或其 IP 地址；
- switch：参数选项，它是下列可选项的组合。

```
[-dfnqrvR][-c count][-i wait][-l preload][-p pattern][-s packtssize]
```

如表 3.6 所示为这些可选参数的含义。

表 3.6　ping 的可选参数

选　项	含　　义
-d	设定后面的测试参数
-f	洪泛 ping——快速发出测试分组。只有超级用户可以选用此项
-n	只输出数字
-q	不显示任何传输分组的信息，只显示最后结果
-r	绕过正常的路由表，通过附加网络直接到达一台主机
-v	详细输出
-R	报告路由
-c	发送指定数目的分组后停止
-i	设定发送测试分组的时间间隔（秒数），预设值为 1（每秒发送一个分组）
-l	预设在故障进入常规行为模式前，ping 能够尽快送出的分组数量。此项仅超级用户可用
-p	规定填充字符
-s	指定分组的数据部分大小（字节数）。预设值为 56（加上 8B 的 ICMP 头，共 64B）

2）Traceroute

Traceroute 程序用来确定通过网络的路由 IP 数据分组。它先把一个 TTL=1 的 IP 分组发送给目的主机，在经过第 1 个路由器时把 TTL 减到 0，遂丢弃该分组并把 ICMP 超时消息返回给源主机，从而标识了第 1 个路由器。以后，不断增加 TTL 值重复上述过程，就可以依次标识出通向目的主机的路径上的各路由器。

3.3　IPv6

3.3.1　IPv4 面临的问题

Internet 最先出现在 20 世纪 60 年代。当初的建造者们怎么也没有想到，它的发展能够如此迅猛，应用的领域能够如此广泛；也没有想到，如此迅速的发展和广泛的应用，也给 Internet 自己带来了无法回避的严重问题。

1．IP 地址空间问题

随着 Internet 的广泛应用和用户数量的急剧增加，只有 32 位（地址数量为 4.3×10^9）的 IPv4（IPv1～IPv3 从来没有被正式使用过，IPv5 仅用来命名 Internet 面向连接的协议 STP）地址危机已经展现在人们眼前。

2．QoS 保证问题

服务质量（Quality of Services，QoS）通常是指通信网络在承载业务时为业务提供的品质保证。不同的通信网络对于 QoS 的定义不同。数据网络的 QoS 通常用业务传输的延迟、延迟变化、吞吐量和丢包率来衡量。

IPv4 采用无连接的分组转发方式传输数据。它的分组转发采取了“尽力而为”的机制。这样的机制，对于流量较少、对实时性要求不高的应用来说，没有多大问题。但是，随着数据流量的增加（如多媒体数据），传输延迟就会明显，信息传输就会出现中断现象。图 3.19 表明当 A 和 B 都有数据要通过 Internet 传输到 C 时，分组就会出现间断现象。

IPv4 主要用于数据传输。随着多媒体业务的兴起，语音和视频也开始在 Internet 上传输。而语音和视频业务要求一定的连续性、相关性和实时性，对网络的 QoS 有较严格的要求，这是目前的 Internet 难以保证的。

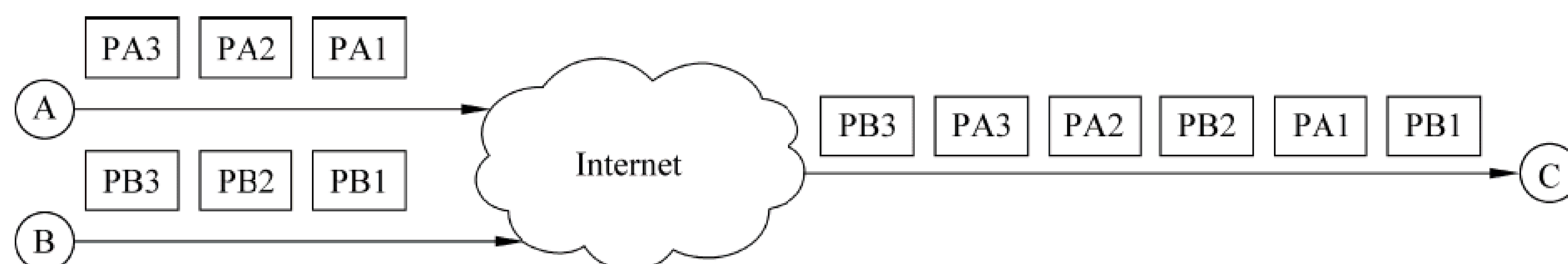


图 3.19　Internet 传输出现的分组间断现象

3．与新标准、新协议兼容问题

当初的 Internet 以高效率为目标，为了提高结点处理数据包的速度，网络结点根据数据

包头的内容对数据包进行一致性处理。而 IP 数据包的包头中虽然有几个可选项，但基本上是固定的。这虽然简化了结点的协议处理，但增加了容纳新标准、新协议的困难度。

4．移动通信设备的连接问题

目前的 Internet 中，主机的 IPv4 地址与其地理位置（网络）有关，这就为移动设备的连接带来困难。

5．安全问题

当初的 Internet 主要面向教育、科研服务，并且以信息共享为宗旨，对管理和安全考虑不足。随着其应用范围的扩大，安全的脆弱性迅速暴露。

为了解决上述问题，IETF 提出了新一代 IP，即 IPv6。

3.3.2 IPv6 地址结构

IPv6 的地址是一个 128 位二进制数组成的地址，即使用点分十进制写，也是相当长的。例如：

10.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255

为了减少地址的书写长度，便于记忆，IPv6 的设计者们建议使用一种更紧凑的书写格式——冒分十六进制表示法（colon hexadecimal notation）。这样，上述地址就可以记为

69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF

在此基础上，人们又提出压缩零（zero compression）表示法。例如：

69DC:0:0:0:0:0:0:B1

可以压缩地表示为

69DC::B1

3.3.3 从 IPv4 向 IPv6 的过渡

随着 IPv4 地址即将枯竭，如何从 IPv4 转向 IPv6，即从 IPv4 向 IPv6 过渡的问题越来越突出。但是由于 IPv6 与 IPv4 不兼容，这一转换过程有许多困难。目前，IETF 的研究从 IPv4 向 IPv6 过渡的专门工作组已经提出了许多方案，这些方案主要有以下几类。

1．双协议栈技术

如图 3.20 所示，IPv6 与 IPv4 虽然格式不兼容，但它们具有功能相近的网络层协议，都基于相同的物理平台，而且加载于其上的 TCP 和 UDP 完全相同。因此，如果一台主机能同时运行 IPv4 和 IPv6，就有可能逐渐实现从 IPv4 向 IPv 6 过渡。

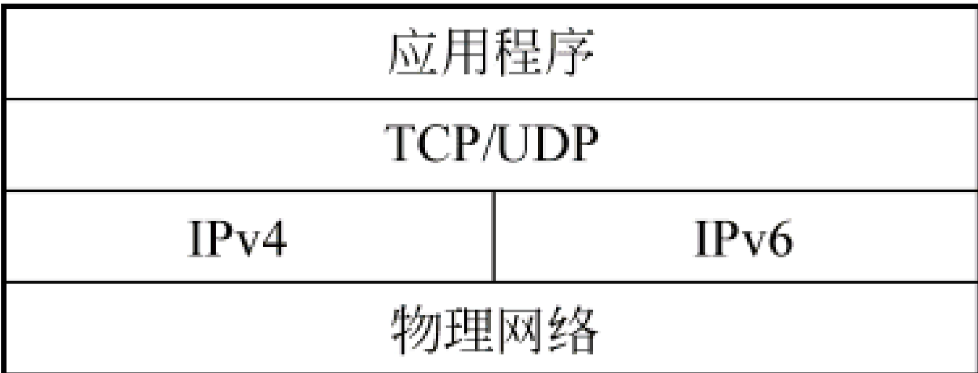


图 3.20　IPv4/v6 双协议栈的协议结构

2．网络地址转换-协议转换（NAT-PT）技术

NAT-PT（Network Address Translation-Protocol Translation）技术通过与 SIIT 协议转换和传统的 IPv4 下的动态网络地址转换（Network Address Translation，NNAT）以及适当的应用层网关（Application Layer Gateway，ALG）相结合，实现只安装了 IPv6 的主机与只安装了

IPv4 的主机间大部分应用的相互通信。

3．6 over 4 隧道技术

随着 IPv6 标准的推广，IPv6 的实验网络已经遍布全球。隧道技术就是设法在现有的 IPv4 网络上开辟一些“隧道”将这些局部的 IPv6 网络连接起来。具体方案是，将 IPv6 数据分组封装入 IPv4，送入隧道，IPv4 分组的源地址是隧道入口，IPv4 分组的目的地址是隧道出口。IPv4 分组穿过隧道后，在出口处再取出 IPv6 分组转发给目的站点。由于隧道技术只在隧道入口和出口处进行修改，因此实现起来比较容易。但无法实现 IPv6 主机与 IPv4 主机间的直接通信。

4．6 to 4 隧道技术

6 to 4 隧道技术简称 6 to 4 技术，它是一种自动构造隧道的技术。它在 IPv4 NAT 协议中加入对 IPv6 和 6 to 4 的支持，成为一个非常吸引人的方案。6 to 4 的关键是它可以自动从 IPv6 地址的前缀中提取一个 IPv4 地址。这样，当用隧道将一个 IPv6 的出口路由器与其他 IPv6 域建立连接时，IPv4 隧道的末端就能从 IPv6 的地址中自动提取出来，从而在 IPv4 的海洋中将各个 IPv6 孤岛相互连接。

3.4 IP 路 由

路由是 IP 层的核心职能。它涉及路由表、路由算法和路由协议，并由路由器实现。

3.4.1 路由器及其工作流程

1. 路由器的作用

在第 2 章曾简单介绍了路由器的基本功能。这里进一步展开介绍。

（1）连通不同的网络。路由器位于不同网络的边界处，起异种网络互连与多个子网互连的作用。另一方面，也可以把一个网络连接到 Internet 或其他广域网络。如图 3.21 所示为将一个园区网接入到 Internet 的实例。

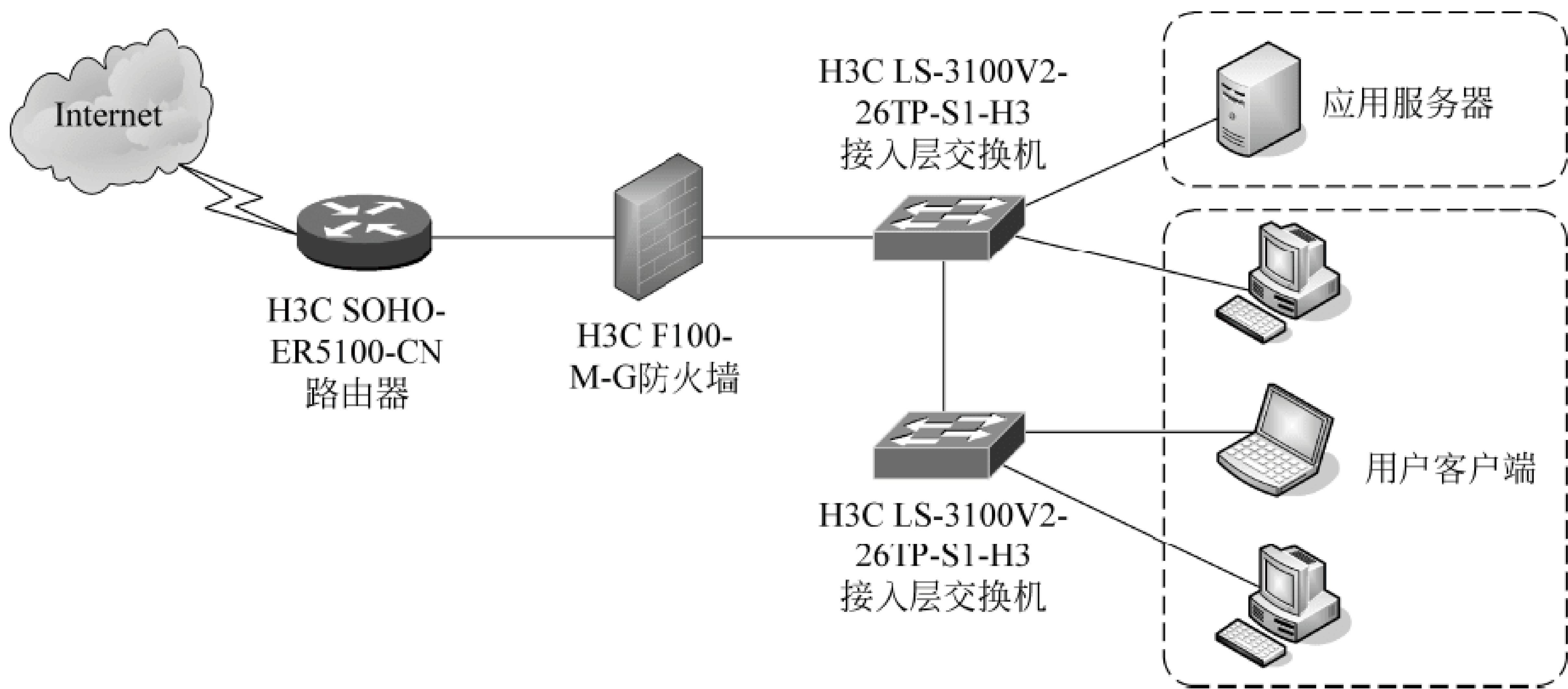


图 3.21　通过路由器接入 Internet 的实例

（2）路由——选择信息传送的路径。路由器工作在网络低 3 层的设备，其主要工作就是为经过路由器的每个数据包寻找一条合适的传输路径，将该数据有效地传送到目的站点。也就是说，其对分组进行转发的依据是 IP 协议规定的网络地址，而不像交换机那样依据的是主机的物理地址。进一步说，它就是执行适当的路由协议。

（3）隔离广播、划分子网。在物理网中传播的帧，可以分为 3 种：单播帧、多播帧和广播帧。单播帧属于“点对点”通信；多播帧可以理解为一个人向多个人（但不是在场的所有人）说话，这样能够提高通话的效率；广播帧就是发向网内所有站的帧。目的 MAC 地址是“FF.FF.FF.FF.FF.FF”的帧就是广播帧。

广播帧并非完全人工所为，病毒、网卡损坏、网络环路等，都可能产生广播帧。当大量广播帧同时在网络中传播时，就会发生很多的数据包的碰撞。而网络为了缓解由于这些碰撞造成的发送失败，就要重传更多的数据包，导致更大量的广播流，从而使网络可用带宽减少，并最终使网络失去连接而瘫痪。这一现象称为广播风暴。

但是对于广播帧，交换机执行的操作是将之转发到所有端口。所以交换机可以分隔冲突域，减少碰撞，但不能避免或减少广播流。抑制广播风暴的基本方法是隔离广播域。显而易见的解决方法是限制以太网上的结点，这就需要对网络进行物理分段。路由器能将不同的用户划分到各自的广播域中。或者说，将网络进行物理分段的传统方法是使用路由器。如图 3.22 所示为使用路由器将一个网络划分为几个子网的实例。

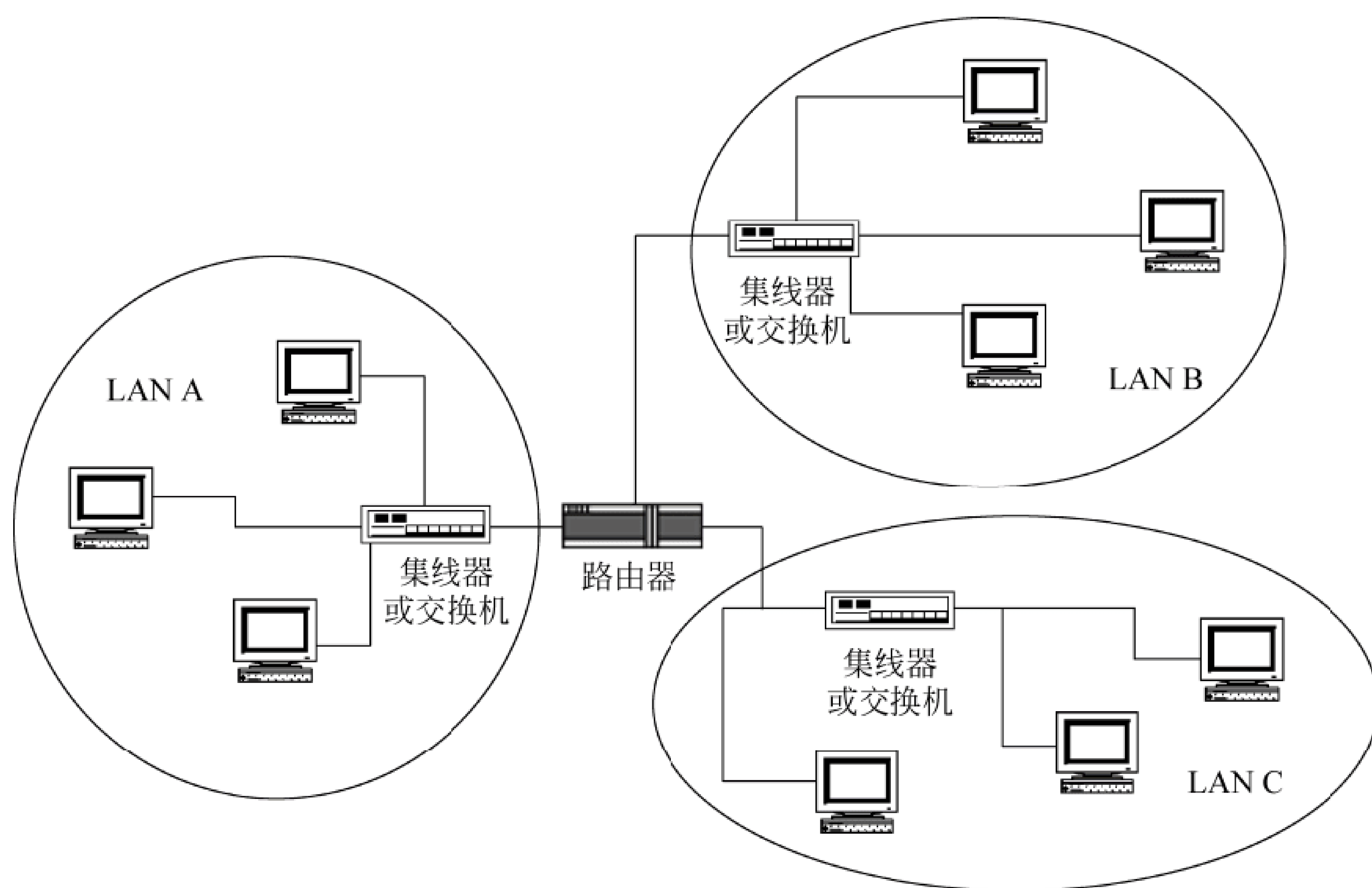


图 3.22　用路由器划分子网

2. 路由器工作流程

如图 3.23 所示为路由器的工作流程。

下面分别介绍路由器工作流程中各步所进行的工作。

① 接收帧，分解出 IP 分组。当封装有 IP 分组的数据帧沿某个物理网传送到路由器的

某个端口时，路由器的低层驱动程序按照相应的数据链路协议接收这个帧，并从中分解出 IP 分组交给 IP 层处理。

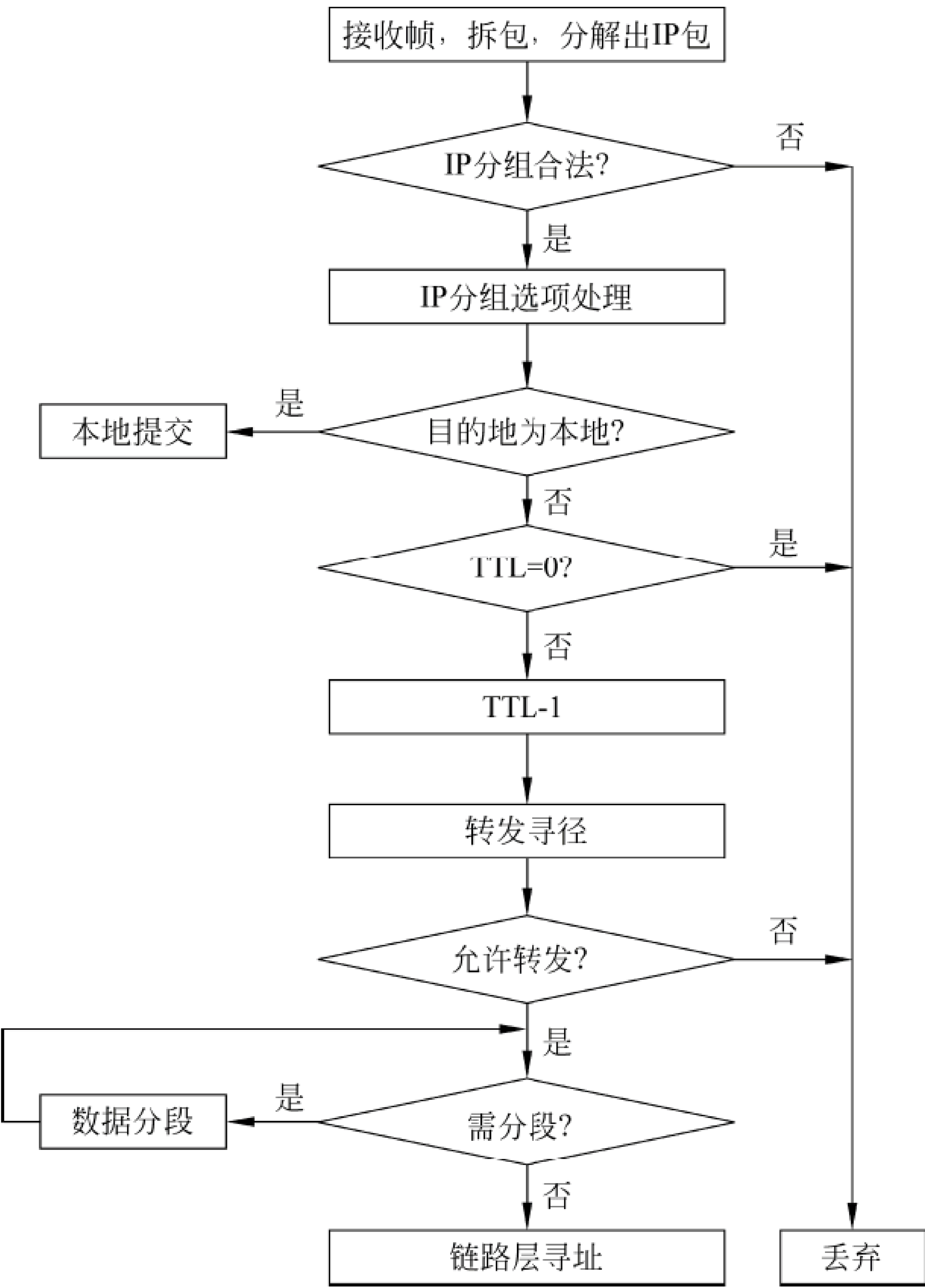


图 3.23　路由器工作流程

② 验证 IP 分组的合法性。对 IP 分组按下列项目进行合法性验证：

- 帧的长度必须能容纳下 IP 分组；
- IP 校验和正确；
- 目前 IP 版本号为 4；
- IP 报头长度必须足够大，可以容纳下最小的 IP 分组（20B）；
- IP 分组必须足够大，要能容纳下 IP 分组头。

③ IP 分组选项处理。根据不同的路由选项类型，路由器在选项数据域中写入不同的内容：

- 记录路由选项，写入自己的 IP 地址；
- 时间戳选项，写入自己的 IP 地址以及当前世界标准时间计算值（以毫秒为单位）；
- 源路由选项，先写入自己的 IP 地址，然后做进一步处理。

④ 确定 IP 分组是本地提交还是转发。

路由器收到一个 IP 分组有三种处理方式：

- 转发，IP 分组中含有一个源路由选项时；
- 本地提交，IP 分组的目的地址或非转发组播地址中的一个与路由器一个端口地址相符；
- 既转发又提交，IP 目的地址是广播地址或是一个组播地址时。

⑤ TTL 处理。生存时间（Time to Live，TTL）用于限制数据包的生存时间，由一个倒计时时钟控制。通常数据包每经过一个路由器，该时钟减 1。当 TTL＝0 时，传送超时，该数据包即被丢弃。

⑥ 转发寻径。IP 选择路由是基于目的网络号，而不是基于目的主机。一个路由表包含许多（N,G）对，N 是目的 IP 网络号，G 是通过路由表可以将 IP 分组送到网络 N 的网关（连接物理网络的路由器）的 IP 地址。当收到一个 IP 分组时，首先通过网络掩码屏蔽操作从目的 IP 地址中找出目的网络号，接着按目的网络号在路由选择表中查找匹配的表项：

- 未找到相匹配的表项时，把该 IP 分组放入默认的下一路径的对应发送缓冲区中排队输出。
- 若找到，则把该 IP 分组放入路由选择表指定的发送缓冲区中排队输出。

⑦ 转发验证。在转发数据分组之前，路由器要有选择地进行一些验证工作，提供一定的安全措施，防止外部主机伪装成内部主机的攻击，如：

- 将 IP 源地址和目的地址不合法的数据分组丢弃；
- 将非法广播和组播数据分组丢弃；
- 通过设置分组过滤和访问列表功能，限制某些方向上的数据分组转发。

⑧ 数据分组分段。当要转发的 IP 分组长度大于输出到的物理网络的 MTU（Maximum Transfer Unit，最大传输单元）时，路由器就要对该数据分组分段。分段的原则是提高网络的传输效率，节省带宽，并有利于提高传输路径上路由器的处理效率。Internet 中常用的分段方法有：

- 第 1 段取当前路径上最有效的 MTU，其余平均分配在比 MTU 小一些的段中，这样可减少以后的分段操作。
- 按 MTU 大小分段，余下的为最后一段（小于 MTU）。
- 将 IP 分组都分作不大于 576B 的段，这可以减少后面的分段，但会增加网络的传输负荷，也会增加目的主机的计算工作量。

需要说明的是，在路由器初始化时，网络管理员为每个转发的网络都配置了一个相应的端口。由这个端口值，可以得到要输出的网络的物理网络类型和它的 MTU 以及相关驱动程序入口。

⑨ 链路寻址。路由器在完成了 IP 层的功能后，接下来是找一个相应的物理端口将数据包从链路层发送出去。具体实现时，IP 层只要把 IP 分组的总长度、目的物理网络地址、下一站的 IP 地址告诉驱动程序即可。驱动程序把 IP 分组封装在数据链路层的帧中，并利用 ARP 等地址解析协议把 IP 地址转换为物理地址。

3.4.2 路由算法

路由表算法用于描述路由器转发分组的策略。下面介绍几种基本的路由算法。

1．洪泛（flooding）算法

洪泛算法也称扩散式算法。它的基本思想是每个结点收到分组后，即将其发往除分组来的结点之外的其他各相邻结点。可以想象，按照这种算法，网络上的分组会像洪水一样泛滥起来，造成大量的分组冗余，导致网络出现拥塞现象。因此，要限制分组复制的数目。可以有 3 种方法：一是在每个分组的头部设一个计数器，用来统计分组到达结点的数量，当计数器超过规定值（如端到端最大段数）时，将之丢弃；另一种方法是在每个结点上建立一个分组登记表，不接收重复的分组；还有一种方法是只选择距目标结点近的部分结点发送分组。

洪泛算法具有很好的健壮性和可靠性，适用于规模较小、可靠性要求较高的场合。

2．热土豆（hot potato）算法

通常每个结点要为其连接的相邻结点各建一个分组队列。热土豆算法是结点收到一个分组后，为了尽快脱手，要将其放在最短的队列中，而不管该分组的目标结点是什么。

3．固定路由算法

固定路由算法也称查表法，它是在网络的每个结点上都存放一个预先计算好的路由表，给出本结点到所有可能的目标结点的最短路径。如图 3.24 所示为一个固定路由算法的例子。这样，一个结点每收到一个分组，通过查表就可找出相应的转发出口。

(a) 通信子网

后继结点		当前结点					
		1	2	3	4	5	6
目标结点	1	/	1	1	5/6	1	1
	2	2	/	2	3	1	1
	3	3	3	/	3	1/4	1/4
	4	3/6	3	4	/	4	4
	5	5	1	1/4	5	/	5
	6	6	1	1/4	6	6	/

(b) 全路由表

图 3.24　一个固定路由算法的例子

固定路由算法简单、实现容易，选择的是最短路径，但是不适应网络的拓扑变化，当被选路由出现故障时，会影响正常传送。改进的方法是为每个结点提供一个次佳路由，当第一路由失效时，启用次佳路由。

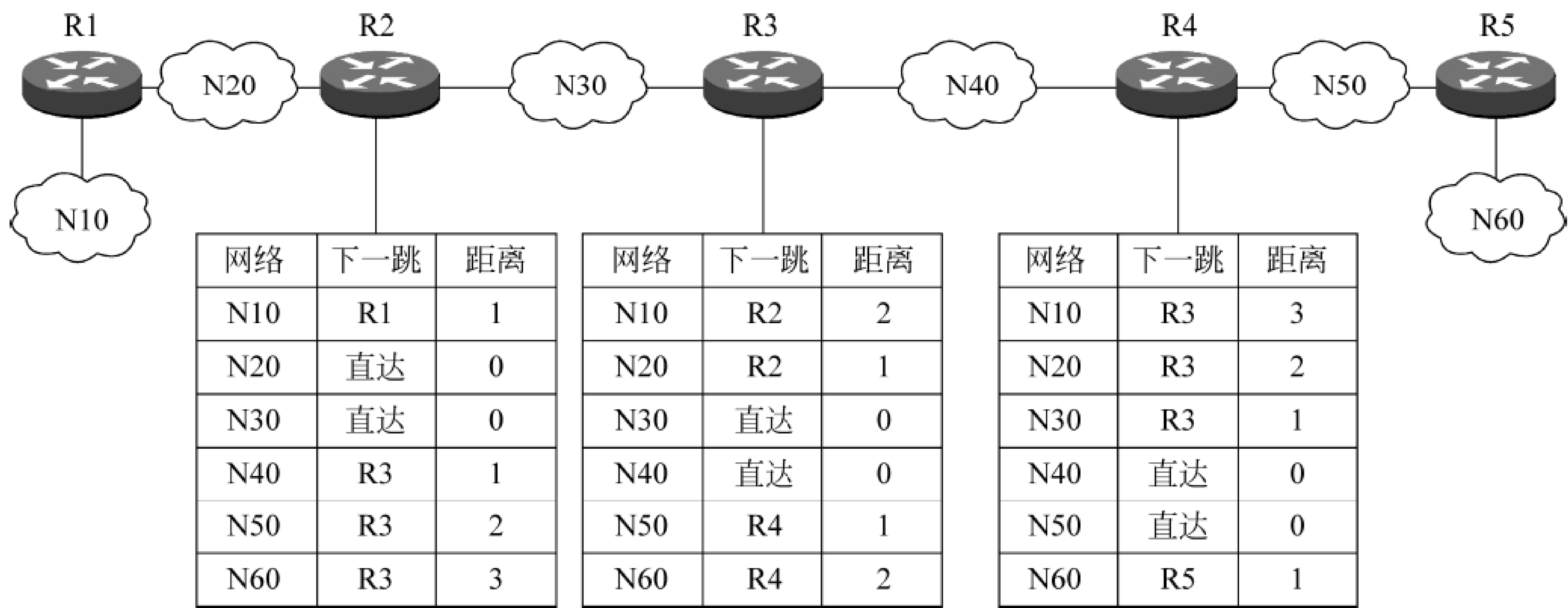
固定的路由是静态路由。当网络的拓扑结构发生变化时，要由网络管理员手工修改路由表中的相关路由。 静态路由信息在默认情况下是私有的，不会传递给其他的路由器，不过，网络管理员也可以将其设置为共享的。

静态路由适合比较简单的网络环境。在这样的环境中，网络管理员易于清楚地了解网

络的拓扑结构，设置正确的路由信息以及网络拓扑变化时进行路由信息的调整不需太多的精力。此外，静态路由具有较高的安全保密性。

4．距离向量（distance vector）算法

距离向量算法的原理非常简单：它把每经过一个路由器称为一跳。一条路由上的跳数称为“距离”，然后动态地选择最短距离作为路径。如图 3.25 所示为一个简单的距离向量路由表示的例子，图中给出了 R2、R3 和 R4 3 个路由器的距离向量路由表。



网络	下一跳	距离
N10	R1	1
N20	直达	0
N30	直达	0
N40	R3	1
N50	R3	2
N60	R3	3

网络	下一跳	距离
N10	R2	2
N20	R2	1
N30	直达	0
N40	直达	0
N50	R4	1
N60	R4	2

网络	下一跳	距离
N10	R3	3
N20	R3	2
N30	R3	1
N40	直达	0
N50	直达	0
N60	R5	1

图 3.25　距离向量路由示例

距离向量算法的主要优点是易于实现和调试，主要用于小型网络中。

3.4.3　路由表

1．路由表及其结构

路由器的主要工作就是为经过路由器的每个分组寻找一条合适的传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表（routing table）。路由表或称路由信息库（Routing Information Base，RIB）是一个存储在路由器或者联网计算机中的电子表格（文件）或类数据库。

2．路由表的类型

（1）静态路由表。静态（static）路由表是由系统管理员事先设置好固定的路由表，一般是在系统安装时就根据网络的配置情况预先设定的，它不会随未来网络结构的改变而改变。

（2）动态路由表。动态（dynamic）路由表是路由器根据网络系统的运行情况而自动调整的路由表。路由器根据路由选择协议（Routing Protocol）提供的功能，自动学习和记忆网络运行情况，在需要时自动计算数据传输的最佳路径。

3. 路由表结构

路由表为到达的分组提供了所有可以选择的路由信息供选择。一条路径作为路由表中的一项。一般说来，路由表中的每项都由以下信息字段组成：

（1）网络 ID，即主路由的网络 ID 或网际网络地址。在 IP 路由器上，有从目标 IP 地址决定 IP 网络 ID 的其他子网掩码字段。

（2）转发地址（下一跳地址）。数据包转发的地址。转发地址是硬件地址或网际网络地址。对于主机或路由器直接连接的网络，转发地址字段可能是连接到网络的接口地址。

（3）端口，即当将数据包转发到网络 ID 时所使用的网络接口。这是一个端口号或其他类型的逻辑标识符。

（4）跃点数（距离）。路由首选项的度量。通常，最小的跃点数是首选路由。如果多个路由存在于给定的目标网络，则使用最低跃点数的路由。某些路由选择算法只将到任意网络 ID 的单个路由存储在路由表中，即使存在多个路由。在此情况下，路由器使用跃点数来决定存储在路由表中的路由。

（5）协议（可选）。适用的协议。

（6）定时（可选）。

表 3.7 为一个路由表示例。

表 3.7　一个路由表示例

目标网络	端口	下一跳	距离	协议	定时
160.4.1.0	e0		0	C	
160.4.1.32	e1		0	C	
160.4.1.64	e1	160.4.1.34	1	RIP	00:00:12
200.12.105.0	e1	160.4.1.34	3	RIP	00:00:12
178.33.0.0	e1	160.4.1.34	12	RIP	00:00:12

4. 路由表项的类型与排列规则

1）路由表项的类型

路由表由如下 4 种类型的路由项组成。它们的主要区别在于目的网络地址字段。

（1）**直接路由**（direct route）。表项中的目的地址字段中的网络号是本地网络，其下一跳地址为空。若选择这项路由，则不再发往其他路由，直接在本网交付给目的主机。

（2）**特定主机路由**（host-specific route）。目的地址是特定主机地址。如在图 3.26 中，通过特定主机路由保证分组从 A 到 B 是经过 R_3，而不是经过 R_1。

（3）**特定网络路由**（network-specific route）。目的地址是一个网络地址，在图 3.27 中，主机 S 的路由表中指定的是 N_2。通常，路由表中多是这种项。

（4）**默认路由**（default route）。在路由表中已经制定了一部分网络的路由，其余网络必须通过某一路有才能到达，则该路由就是默认路由，在图 3.28 中，除 N_2 外的其他网络必须通过 R2。则该路由就是默认路由。目的地址为 0.0.0.0 的路由是默认路由。

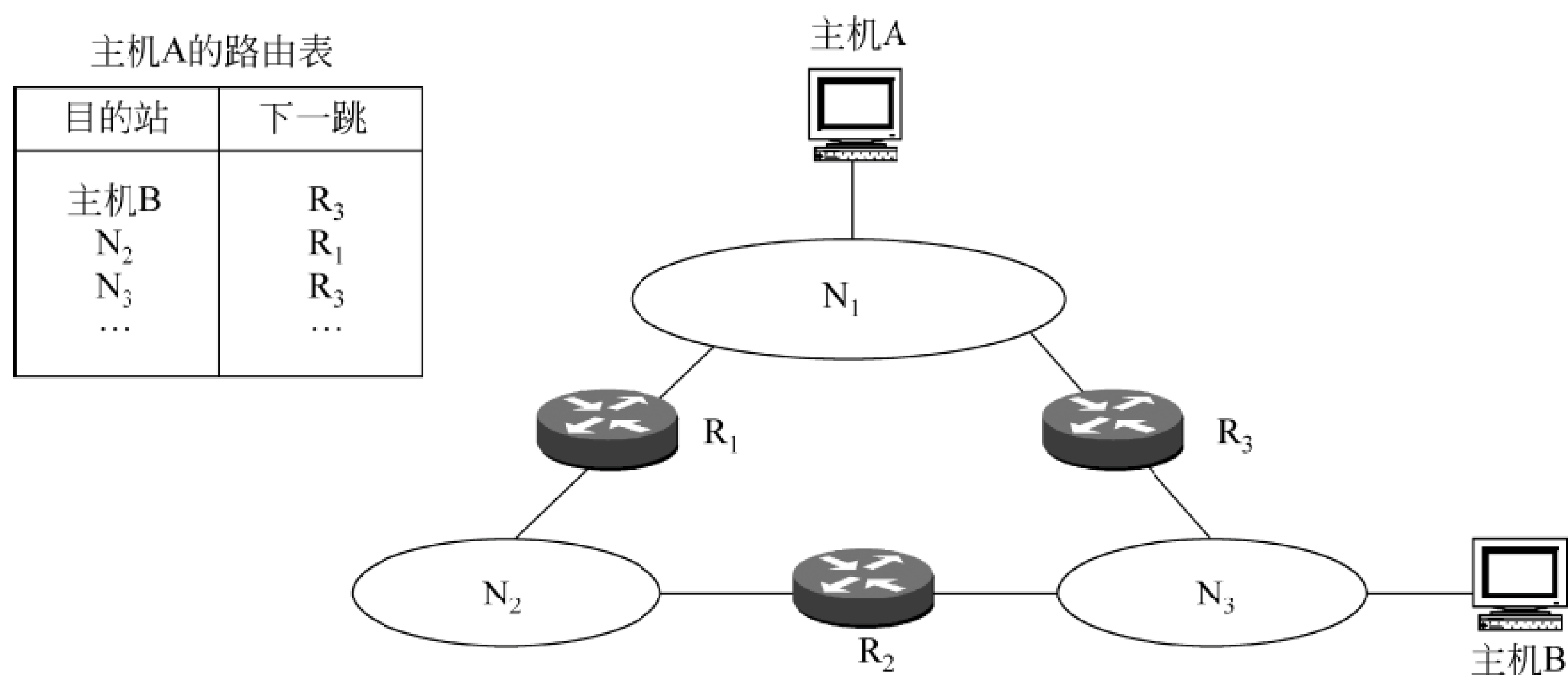


图 3.26　特定主机路由

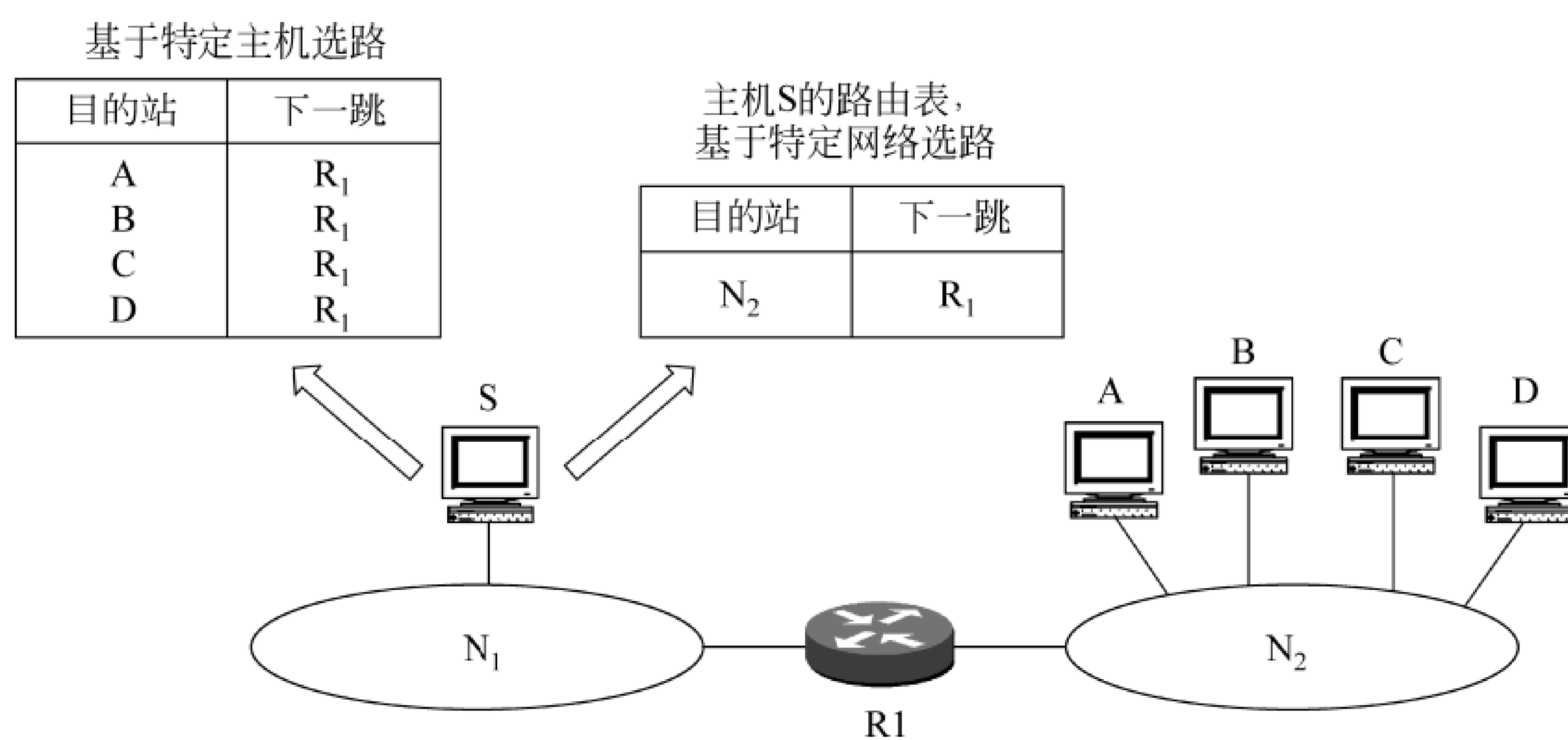


图 3.27　特定网络路由

2）表项在路由表中的排列顺序和选择顺序

在路由表中表项从前到后的排列顺序为：直接路由项、特定主机路由项、特定网络路由项、默认路由项。进行路由选择时，也按照这样的顺序进行，如图 3.29 所示。

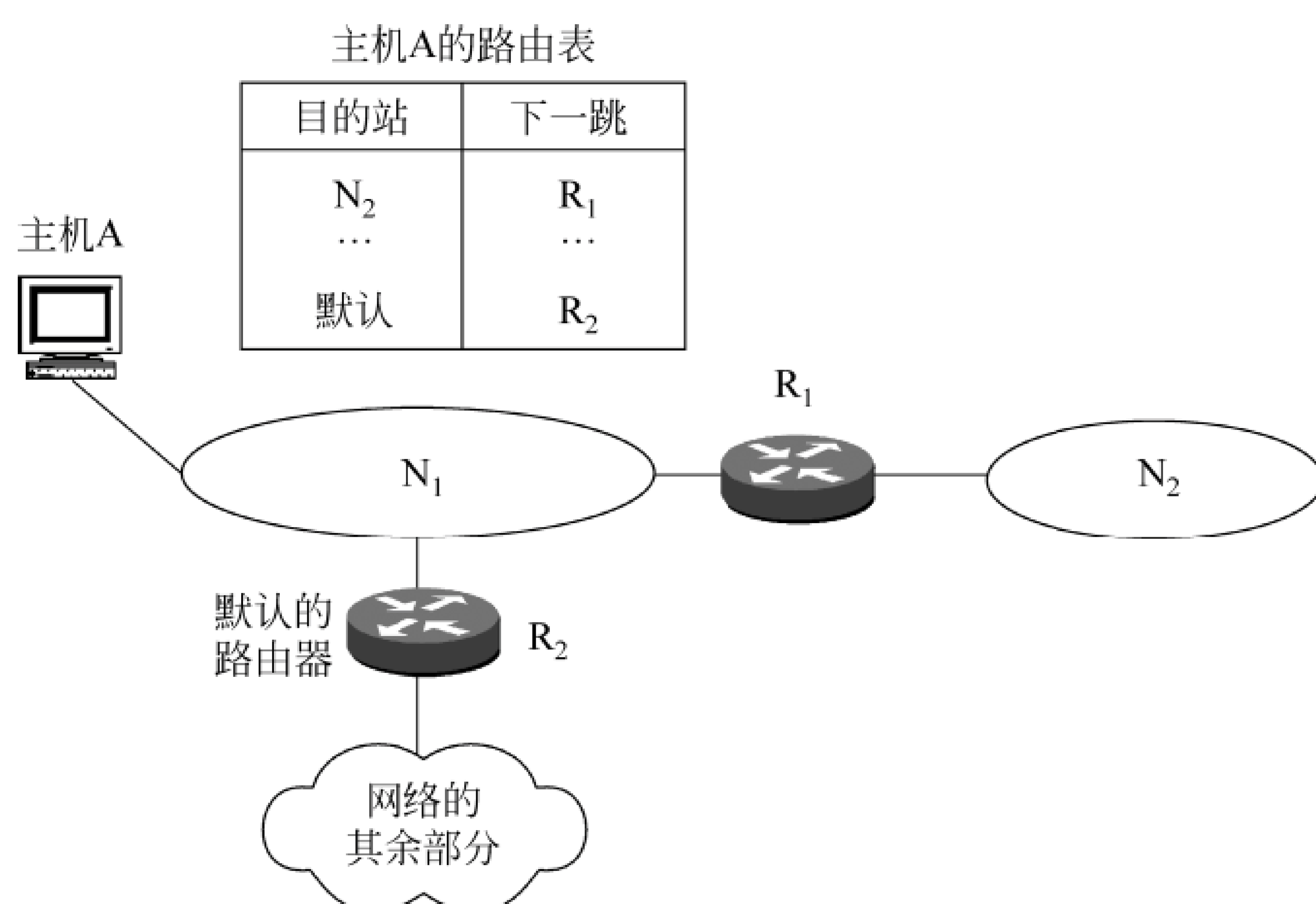


图 3.28　默认网络路由

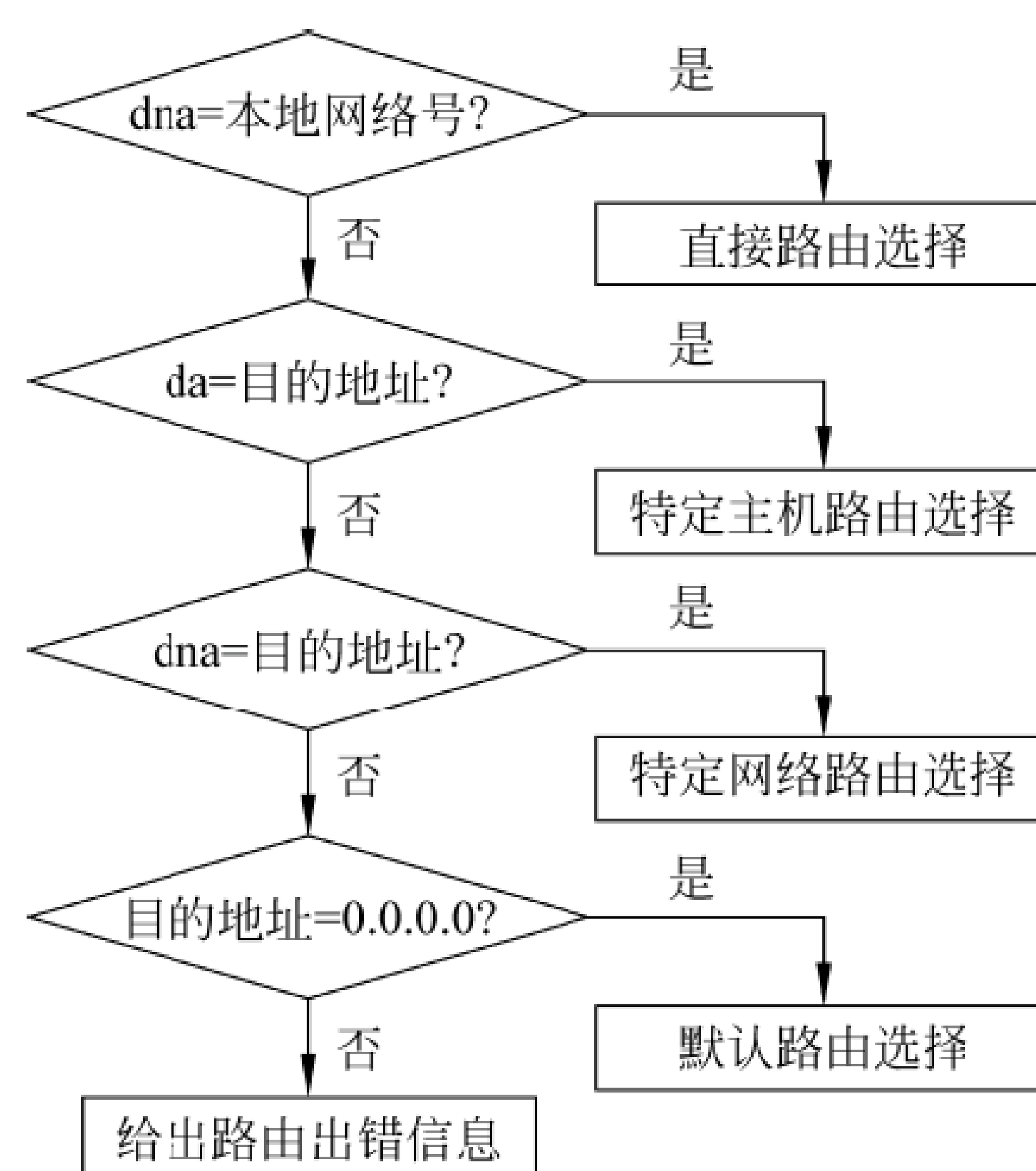


图 3.29　路由表中表项类型选择顺序

3）路由器选择的其他原则

（1）最小地址范围原则，即最长掩码匹配原则。

（2）如果路由表中目的网段的范围相同，则路由优先级高者优先（优先级数值越小，优先级越高）。

（3）如果路由表中目的网段的范围相同，并且路由优先级也相同，则开销（metric）小的优先（metric 值越小，开销越小）。

3.4.4 路由协议

路由算法用于选择最佳路径，它要以相关的路径信息——路径表（routing）为依据。而网络拓扑结构和负荷在不断变化，为了准确地反映这些变化的信息网络路径信息，必须不断在各路由器之间进行信息交换。路由器间相互交换网络信息的规范由路由协议定义。在 Internet 中运行着大量的路由协议，这些协议基本上属于动态自适应、分布式路由选择协议。

由于各 ISP 有自己的利益，不愿意提供自身网络详细的路由信息，因而整个 Internet 不适合遵循单一的路由协议。为了保证各 ISP 的利益，便于进行路由选择，Internet 按运营被划分成许多较小的单位——自治系统（Autonomous System，AS）。每个 AS 通常由一个组织中的互联网络构成，由一个单独的管理机构管理（即由一个 ISP 运营），有权自主地决定本系统内部的路由协议。

划分了自治系统后，就可以把 Internet 中使用的路由协议分为两大类。

（1）内部网关协议（Interior Gateway Protocol，IGP）——在一个自治系统内部使用的路由选择协议与其他自治系统中采用什么路由选择协议无关，主要有 RIP、OSPF 等。

（2）外部网关协议（External Gateway Protocol，EGP）——当两个自治系统中使用不同的路由选择协议时，在两个自治系统之间进行数据报文的转换路由选择协议，主要有 BGP。

1. 路由信息协议

路由信息协议（Routing Information Protocol，RIP）是 IGP 中最早得到广泛应用的协议，其主要优点是简单。

1）RIP 的基本特点

（1）仅与相邻路由器交换信息，即不相邻不交换。

（2）动态更新，定时交换。一个自治系统开始工作时，各路由器首先建立自己的初始路由表；然后周期性地（通常每隔 30s）更新它的距离向量表，及时交换因拓扑结构变化引起的路由信息，维护相邻路由器的关系，同时根据收到的路由表计算自己的路由表。图 3.30 为使用 RIP 建立路由表的过程举例。

（3）层距离向量协议。RIP 以距离（跳数）作路由选择的唯一标准，即使还存在另一条高速（低时延）但跳数较多的路由，也只能按照含最少跳数（hop count）选择路由。因此，它所使用的路由信息是其全部路由表信息。这种设计加上只与相邻路由器交换信息并只定时交换，所以简单，但影响了 RIP 路由协议的收敛，甚至会出现不收敛的现象。

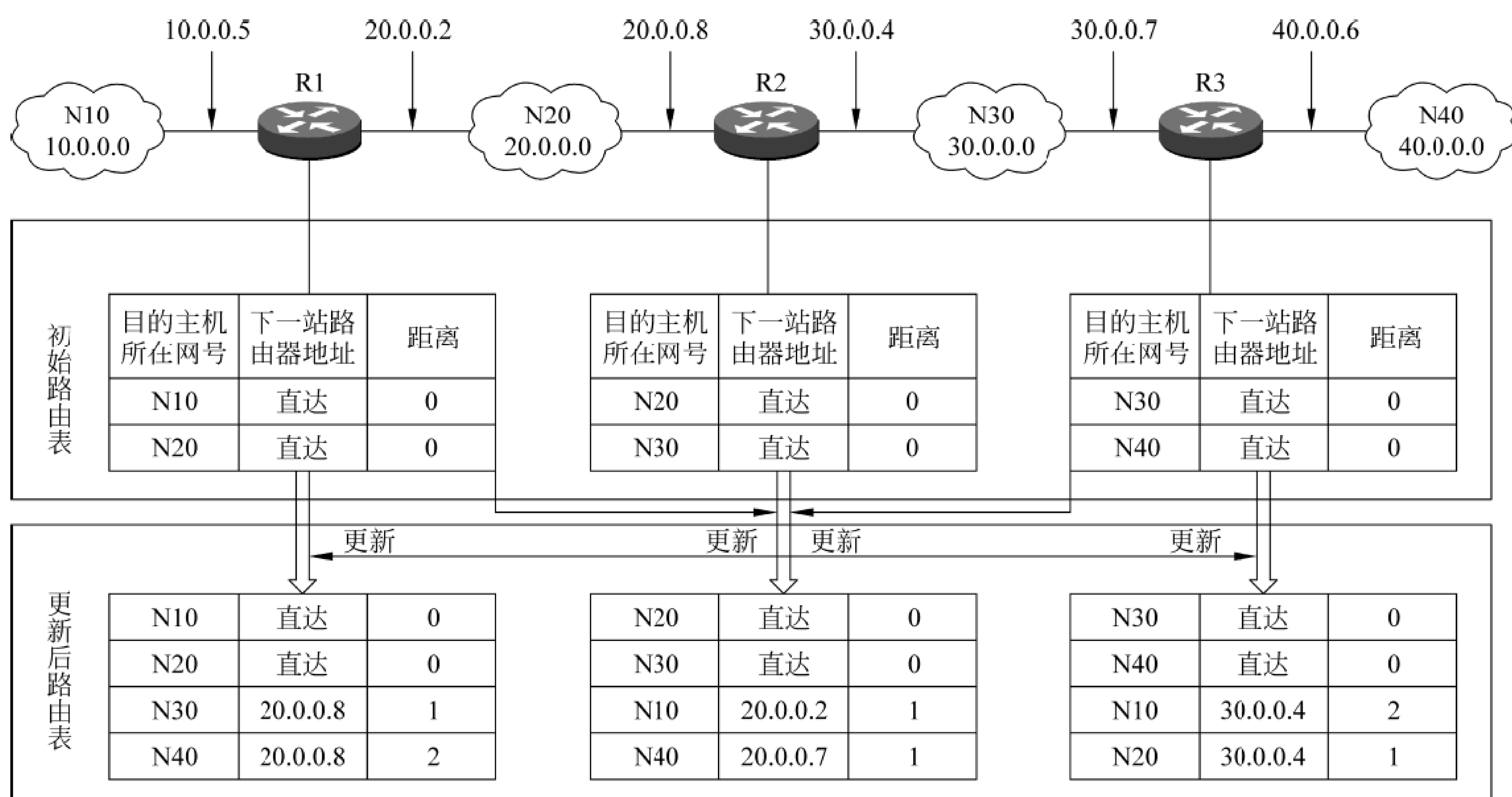


图 3.30　使用 RIP 建立路由表的过程举例

（4）适用于小型自治网络。RIP 实现简单，开销较小，但允许一条路由最多只能包含 15 个路由器。即最多 15 个跳数。当距离的最大值达到 16 时，就称为不可到达。可见 RIP 只适用于小型网络。

（5）好消息传得快，坏消息传得慢。如果路由器发现了一条更短的路由，更新消息就会传播得很快；而当网络出现故障时，由于跳数到达 16 才称为不可到达，所以要经过较长时间才能将此信息传送到所有路径。坏消息传播得慢，会使许多更新过程的收敛时间过长，以及故障在网络中停留时间太长。

2）RIP 报文类型

RIP 通过报文进行信息交换。它有如下两种报文：

（1）请求报文。RIP 请求报文用于查询相邻 RIP 设备，以获得它们的距离向量表。

（2）响应报文。RIP 响应报文由一个 RIP 设备发出，用于公告它的本地距离向量表中维护的信息。这个报文在如下几种情形下被发送：

- 如果网络中没有变化，每隔 30s 自动发送一次更新信息；
- 如果网络有变化，路由器立即发送新的路由表——触发更新；
- 作为对另一个 RIP 结点的请求报文的响应。

当一个 RIP 设备接收到一个响应报文时，便将更新信息与本地距离向量表进行对比。如果更新信息中包含了一条到目的网络的代价更低的路由，则对本地表进行更新。

3）RIP 报文格式

不同网络系统中 RIP 报文的格式是不相同的。在 TCP/IP 协议栈中的 RIP 报文格式已经有了 3 个不同等级的版本：第一版的 RFC 1058(1988)描述了 RIP 的实现；RFC 1723(1994)称作 RIP2，允许分组包含更多的信息并提供了简单的认证机制是它的更新格式；较新的版本是 RFC 2495(1998)，报文格式与 RFC 1723 相同，但性能有所改进。RIP2 的报文格式由首部和一些路由信息表项组成。图 3.31 是首部和每个路由信息表项的格式。

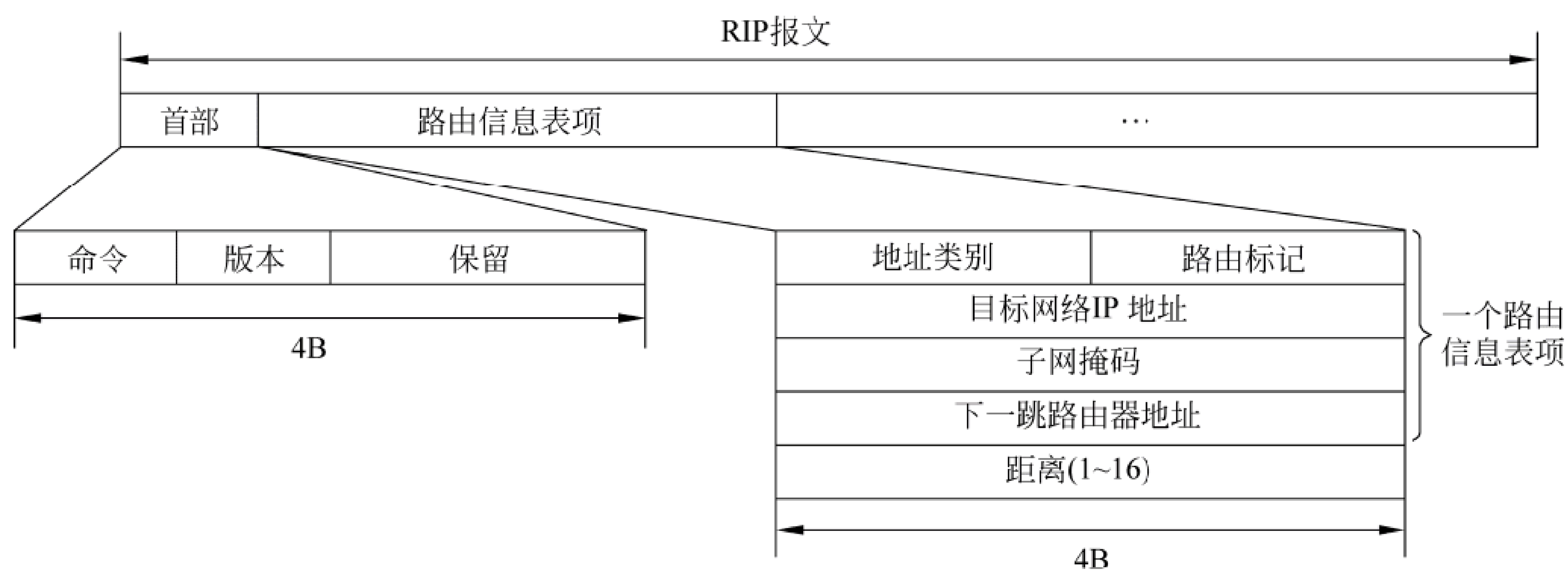


图 3.31　RIP 报文格式

（1）RIP 首部。RIP 报文首部占 4B 字节，包含 3 部分内容：命令、版本号和保留。

- 命令字段指出报文的含义，如：1——请求路由信息；2——对请求路由信息的响应或未被请求而发出的路由更新报文。
- 保留字段全为 0，用于填充成 4B。

（2）路由部分。路由部分由一些路由信息表项组成。每个信息路由表项占 20B，包含 6 个字段：

- 地址类别：用来标志所使用的地址协议。如采用 IP 地址，其值为 2。
- 路由标记：填写自治系统的标识号，以便接收本自治系统之外的路由选择信息。
- 其他 4 个字段分别为某个目的网络的网络地址、子网掩码、下一跳路由器地址和到此网络的距离——跳数（1～16）。RIP 允许一条路径最多包含 15 个路由器，再用一个 16 表示不可到达。

在一个单独的 RIP 通知中最多可以发送 25 个路由信息表项。超过 25 个路由，必须另外用一个 RIP 报文传送。

2. 开放式最短路径优先协议

1）OSPF 的设计特点

OSPF（Open Shortest Path First，开放式最短路径优先协议）是针对 RIP 的缺点于 1989 年开发出来的一种内部网关协议（Interior Gateway Protocol，IGP）。所谓内部，是指仅作用于单一自治系统内决策路由；所谓“开放”，是指它不受任何一家厂商所左右，这正是它的强大生命力和广泛用途的源泉所在；所谓“最短路径优先”是为了表明它采用了 Dijketra 最短路径算法。此外，与 RIP 相比，它还有下列几个特点。

（1）OSPF 是链路状态协议。它把物理网络称为链路，路由器作为链路的连接结点，它维护的是一张网络有向拓扑图。所发送的信息是本结点（路由器）所连接的各链路的状态，并且仅当链路状态发生变化时才进行信息交换，而不是定时信息交换。

（2）信息交换时采用洪泛算法，向所有的结点发送信息，而不是只向相邻接点发送信息。

（3）分层路由。为了适应规模很大的网络，OSPF 把一个大型网络除了按照运营分割成一些自治系统外，还进一步分割成一些“区域”(area)，形成不同层次的路由：

- 同一区域中的路由器只在该区域内部交换 LSA（Link-State Advertisement，链路状态通告）信息；
- 不同区域间的路由器通过区域边界的路由器进行汇总，并与其他区域交换 LSA 信息。

这样 LSA 报文数量及链路状态信息库表项都会极大减少，从而大幅度地改善了网络的可扩展性，加速了路由选择的收敛速度。

（4）OSPF 路由协议支持路由验证，只有互相通过路由验证的路由器之间才能交换路由信息。并且 OSPF 可以对不同的区域定义不同的验证方式，以提高网络的安全性。

2）OSPF 区域

OSPF 针对 Internet 中许多 AS 很庞大、不便于管理的情形，将每一个 AS 分为一些编号区域（area），每个区域是包含在 AS 内部的一些网络、主机、路由器的集合，通常对应地理边界或者行政边界。每个区域由一个唯一的区号定义，这个区号配置在每一个路由器内。定义了相同区号的路由器接口成为相同区的组成部分。区域是通过一个 32 位的区域 ID 来识别的。区域 ID 可以表示成一个十进制的数字，也可以表示成一个点分十进制的数字，例如：

0～0.0.0.0

16～0.0.0.16

271～0.0.1.15

OSPF 网络中能支持的区数量受限于区 ID 的大小。32 位二进制数对应的最大十进制数为 4 294 967 295。单个区域所支持的路由器最大数量的范围大约为 30～200。但在一个区域内实际加入的路由器数量要比单个区域所能容纳的路由器最大数量小一些。

所有的 OSPF 网络都要包含一个区域。区域的引入，使同一个 AS 内的所有路由器不再都有一个相同的链路状态数据库，而是仅仅同一区域的路由器具有相同的链路状态数据库，使数据库的大小缩减，链路状态数据库的减小也就意味着处理较少的 LSA 通告，从而也就降低了对路由器 CPU 和内存的消耗。对于每一个区域，其网络拓扑结构在区域外是不可见的。同样，在每一个区域中的路由器对其域外的其余网络结构也不了解。由于链路状态数据库只需要在一个区域内进行维护，因此，大量的 LSA 洪泛也将被限制在一个区域内。

在 OSPF 网络中，要有一个主干区域（backbone area）。主干区域一般为区域 0。在具有多个区域的 OSPF 网络中，主干区域要与其他区域连接，以使其他区域直接把路由信息通知给主干区域，然后再由主干区域把此信息通知给其他区域。因此，主干区域相当于一级区域，其他区域相当于二级区域。因此，所有的区间路由必须经过区域 0 传输，不允许非 0 区域直接和其他区域通信。这个层次限制确保了 OSPF 具有良好的可扩展性，而不会导致链路和路由器的混乱。

3）OSPF 路由器分类

在 OSPF 路由协议中，路由器按照其所处的位置可以分为 4 类。

（1）内部路由器（internal router）：只连接一个区域内网络的路由器，其所有定义接口属于同一区域，但这个区域不是 0 区域。

（2）区域边界路由器（Area Border Router，ABR）：连接不同区域的路由器，可以把本

区域的有关信息概括起来发给其他区域。

（3）自治系统边界路由器（Autonomous System Border Router，ASBR）：连接 AS 的路由器。

（4）主干路由器（backbone router）：主干路由器是至少有一个接口定义为属于区域 0 的路由器。一个主干路由器同时也可能是一个 ABR 或 ASBR：一个区域边界路由器也可能是一个主干路由器。任何一个与区域 0 互联的区域边界路由器也将成为主干路由器。

图 3.32 是一个具有 4 类路由器的例子。这是一个只有 3 个区域的相当简单 OSPF 网络，这 3 个小区的编号为 0、1 和 2，主干区域编号为 0。

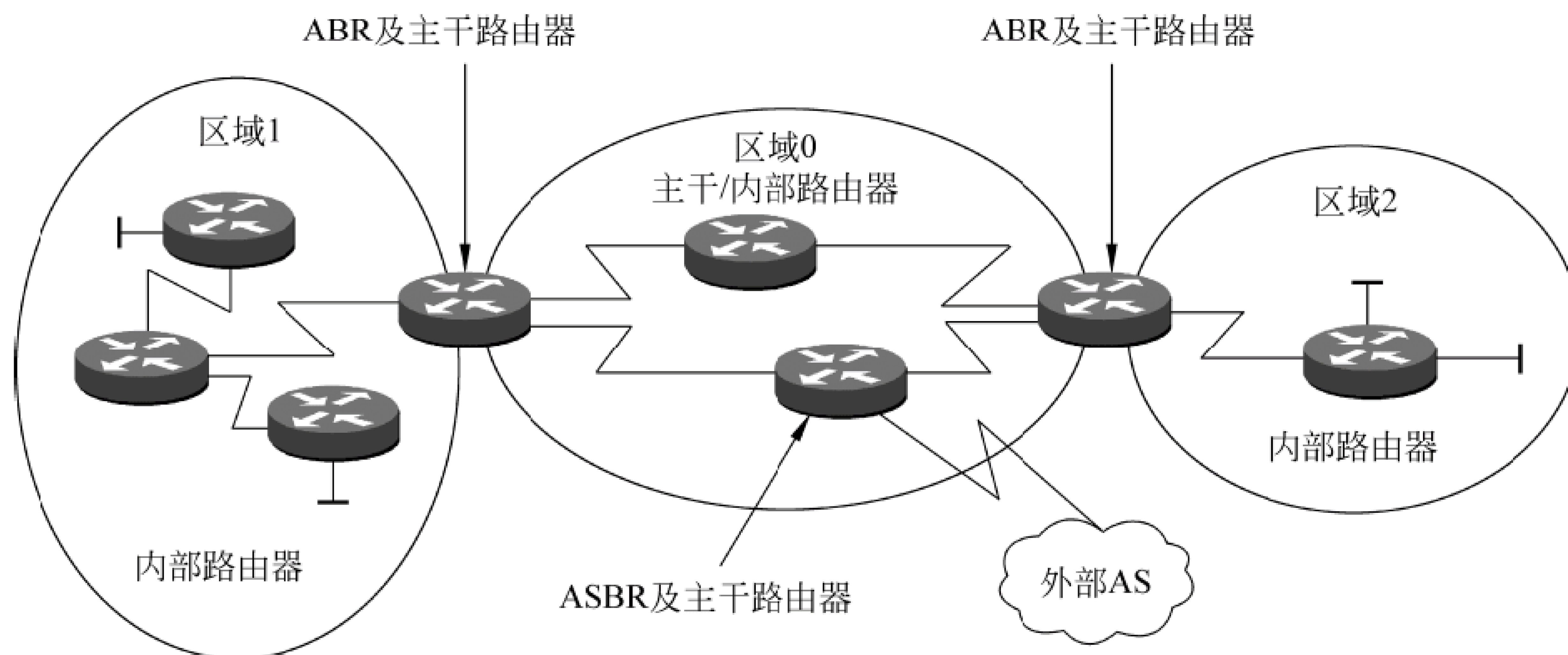


图 3.32　一个具有 4 类路由器的例子

4）OSPF 链路（网络）类型

OSPF 把物理网络称为链路。目前已经定义了 4 种类型的链路。

（1）点到点链路（或称点对点网络）：直接连接两个路由器，中间没有其他主机或路由器。

（2）多路访问（Multi-Access）网络（链路）也称过渡链路，是一种连接有若干个路由器的网络。数据可以从任何一个路由器进入网络，并从任何另一个路由器离开。这种链路又可以分为两种：

- 广播多路访问链路（网络）。支持与两个以上的路由器连接，并可以同时把一个报文发送到所有与之连接的路由器。
- 非广播多路访问链路（网络）。支持与两个以上的路由器连接，但无广播能力。其特例是点到多点链路（网络）。

（3）残桩（Stub）链路：只连接到一个路由器的网络。数据分组通过这个单一路由器进入网络，并通过这个路由器离开该网络。

（4）虚拟链路。OSPF 要求所有区域必须与主干网络连接。如果某个区域边界路由器与主干路由器之间的链路断开，那么管理员会在它们之间使用一条更长的路径（可能经过几个路由器）虚拟链路，将之连接起来。

5）邻接路由器和 OSPF 报文类型

属于相同 OSPF 区域的两个相邻路由器（neighbor router），在同步了它们的拓扑结构数据库后，就可以成为邻接路由器。OSPF 通过邻接路由器交换链路状态信息。为了完成信息

交换，OSPF 定义了如下一些活动：

- 发现邻居；
- 选择一个指定路由器；
- 建立邻接关系；
- 同步数据库。

这些活动通过如表 3.8 所示的 5 类 OSPF 消息完成。

表 3.8　OSPF 的 5 类消息

报文类型	描　　述
Hello 报文	路由器启动时，用于发现邻接路由器
数据库描述报文	出现新链路时，给出报文发送者拥有的所有链路状态项序列号，接收者据此判定谁的数据最新
链路状态请求报文	路由器间相互发送该报文以从邻接路由器要求获取对应的链路状态信息，确定谁的数据最新
链路状态更新报文	用洪泛法向全网发送更新链路数据库状态
链路状态确认报文	对链路更新报文的确认

6）LSA 及其类型

LSA 可以描述一个单独的网络组成成分（如路由器、网段或者外部目标等）。LSA 在 OSPF 的邻接路由器间进行交换，以同步每个设备上的链路状态数据库。它包含如下 5 种主要信息类型。

（1）LSA TYPE 1——路由器 LSA。它们描述本区域路由器链路的状态（链路类型、地址、掩码等）、沿每条链路方向出站的代价以及路由器是否是 ABR 或 ASBR。一个边界路由器可能产生多个 LSA TYPE1。这些 LSA 通告只会在始发它们的区域内部进行泛洪，不会穿越 ABR。

（2）LSA TYPE 2——网络 LSA（network LSA），由 DR（Designated Router，指定路由器）产生。DR 是一个区域中可以与所有其他路由器建立相邻关系的路由器，负责收集所有的链路状态信息，并发布给其他路由器，以大大减少需要建立的邻居关系。

DR 通常由优先级别最高的路由器担任。但它不是人工指定的，而是由本网段中所有的路由器通过 Hello 协议选出的。选举方法如下：一个路由器的 Hello 包中有它自己的优先级，这个优先级是在每个端口基本配置时给出的。通常，当到一个网络的一个路由器的端口第一次被激活时，它首先检查网络中是否有 DR：如果有，它接受这个指定路由器，而不管它自己的优先级；如果没有，并且它自己是这个网络中最高优先级的路由器，则宣布自己为 DR。选举 DR 的同时也选举出一个备份指定路由器（Backup Designated Router，BDR），在 DR 失效的时候，BDR 担负起 DR 的职责。

网络 LSA 只在一个区域里传播，不会穿越 ABR。

（3）LSA TYPE 3——网络汇总 LSA（network summary LSA），由 ABR 产生，含有 ABR 与本地内部路由器连接信息，可以描述本区域到主干区域的链路信息。它通常汇总默认路由而不是传送汇总的 OSPF 信息给其他网络，可以在整个 AS 内进行洪泛。

（4）LSA TYPE 4——ASBR 汇总 LSA。由 ABR 产生，由主干区域发送到其他 ABR，含有 ASBR 的链路信息，可以在整个 AS 里进行洪泛。与 LSA TYPE 3 的区别在于 TYPE 4 描

述到 OSPF 网络的外部路由，而 TYPE 3 则描述区域内路由。

（5）LSA TYPE 5——AS 外部 LSA（autonomous system external LSA），或称为外部 LSA（external LSA）。由 ASBR 产生，含有关于自治域外的链路信息，可以在整个 AS 内洪泛。除了存根区域和完全存根区域，LSA TYPE 5 在整个网络中发送。

7）OSPF 数据包格式

每一个 OSPF 报文都由头部和实例（instance）组成。OSPF 头长为 24 个字节，包含如下 8 个字段。

- Version number：定义所采用的 OSPF 路由协议的版本。
- Type：定义 OSPF 数据包类型。
- Packet length：定义整个数据包的长度。
- Router ID：用于描述数据包的源地址，以 IP 地址来表示。
- Area ID：用于区分 OSPF 数据包属于的区域号，所有的 OSPF 数据包都属于一个特定的 OSPF 区域。
- Checksum：校验位，用于标记数据包在传递时有无误码。
- Authentication type：定义 OSPF 验证类型。
- Authentication：包含 OSPF 验证信息，长为 8 个字节。

8）OSPF 的工作过程

① 建立邻接关系。所谓“邻接关系（Adjacency）”，是指 OSPF 路由器以交换路由信息为目的，在所选择的相邻路由器之间建立的一种关系。一个路由器一开始运行 OSPF 协议，就试图与相邻路由器建立邻接关系。它定期地向各个网络（链路）接口（包括虚拟链路接口）发送 Hello 报文。在 Hello 报文中，含有自己的 ID（即某一接口的 IP 地址）、优先权和相邻路由表。接收到 Hello 报文的路由器如果发现自己在对方的相邻路由表中，就表明双方都收到了对方的 Hello 报文，于是它就根据该端口所在网络类型确定是否可以建立邻接关系：

- 若在点对点网络中，路由器将直接和对端路由器建立起邻接关系。
- 若为多路链路，该路由器将进行 DR 选举操作——优先权（Priority）字段值大小为 0～255，优先权值最高的路由器成为 DR；如果优先权值大小一样，则 ID 值最高的路由器选举为 DR。优先权值次高的路由器选举为 BDR。

② 同步 LSA 数据库。建立了邻接关系的路由器之间相互交换各自 LSA 数据库内信息的过程称为数据库的同步。在基于 SPF 的路由算法中，所有路由器的拓扑数据库保持同步是很重要的。

每当路由器发送新的 LSA 时，其序列号将增 1。路由器接收到一个新的 LSA 后，可以根据 LSA 头部的类型、标志和广播路由器判断其自身数据库中是否有相同的 LSA，并根据 LSA 序号决定对哪一个 LSA 更新。

- 假设路由器 A 与路由器 B 刚建立起邻接关系，路由器 A 和 B 将相互发送数据库描述报文。在数据库描述报文中包括多个 LSA 头部。
- 一方（如 B）发现对方（如 A）的数据库描述报文中一些 LSA 头所代表的 LSA 自己的数据库中没有，或比自己的新，则将该 LSA 头部放入自己的 LSA 请求表中，

然后向对方发送链路状态请求报文，要求得到具体的 LSA 信息（实例）。

- 对方（如 A）收到 LSA 请求报文后，将向请求方（如 B）发送 LSA 更新报文。更新报文的数据部分是所请求 LSA 的完整信息。
- 请求方（如 B）收到每一个 LSA 更新报文后，进行检查，将收到的新的 LSA 从自己的 LSA 请求表中删去，并向发送方（如 A）发出 LSA 确认报文。
- 如果两个路由器间的 LSA 请求表为空，则表明两者的数据库达到一致，同步成功。

注意，同步是一个扩散过程。即一个路由器在其链路状态发生变化或收到其他路由器发送的 LSA 更新报文后，也要向其邻接路由器主动发送 LSA 更新报文，以便其他路由器尽快更新其拓扑数据库。

③ 计算路由表。在接收到新的链路状态更新报文以及在实现了数据库同步后，路由器都要根据拓扑数据库重新计算它到各子网的最短路径，建立路径表。计算采用 SPF 算法进行。

由于 OSPF 将 Internet 分成区域、AS 和 AS 外部三个层次，所以路由的计算也要分三个层次进行。

- 根据所在区域的数据库，利用本区域内的路由器 LSA 和网络 LSA，计算路由器到本区域内各网络的路由。
- 根据 ABR 向本区域散发的网络综合 LSA，计算路由器到本 AS 其他区域内各子网的可达信息。
- 根据 ASBR 综合 LSA 和外部 LSA，计算路由器到 AS 外部的网络的可达性。

OSPF 利用量度（cost）计算目的路径 cost 最小者即为最短路径。cost = 100×106/链路带宽。显然，OSPF 的 cost 与链路的带宽成反比，带宽越高，cost 越小，表示 OSPF 到目的地的距离越近。

④ 维护路由信息。当链路状态发生变化时，OSPF 通过刷新过程通告网络上其他路由器。OSPF 路由器接收到包含有新信息的链路状态更新报文，将更新自己的链路状态数据库，然后用 SPF 算法重新计算的路由表。在重新计算的过程中，路由器继续使用旧路由表，直到 SPF 完成新的路由表计算。新的链路状态信息将发送给其他路由器。值得注意的是，即使链路状态没有发生改变，OSPF 路由信息也会自动更新，默认时间为 30 分钟。

9）SPF 算法及最短路径树

上面提到，OSPF 的每个路由器都要使用 SPF 算法计算是 OSPF 路由协议的基础。SPF 算法有时也被称为 Dijkstra 算法，这是因为最短路径优先算法 SPF 是 Dijkstra 发明的。SPF 算法将每一个路由器作为根（ROOT）来计算其到每一个目的地路由器的距离，每一个路由器根据一个统一的数据库会计算出路由域的拓扑结构图。该结构图采用树结构，在 SPF 算法中被称为最短路径树。在 OSPF 路由协议中，最短路径树的树干长度，即 OSPF 路由器至每一个目的地路由器的距离，称为 OSPF 的 cost，其算法为：从源结点开始，将所连接的结点分为两个集合——试验的和确定的，即先将一些结点选入试验结点集合中，然后检查它们，并把符合给定准则的结点移入确定结点集合中，从而找到最短路径中的一个结点。重复进行，直到到达目的结点。下面说明算法。

（1）以本地结点（路由器）作为树根。

（2）将代价 0 指派给该结点，并使之成为确定结点。

（3）重复进行下列步骤，对最后一个确定结点的每一个相邻结点进行检查，直到找到最短路径：

- 给每一个结点指派一个累计 cost，并使之成为试验结点；
- 在试验集合中寻找具有最小累计 cost 的结点，使其成为确定结点。

3. 边界网关协议

边界网关协议（Border Gateway Protocol，BGP）是一种外部网关协议。其开发初衷是提供一种自治系统之间交换路由信息的非循环方法，它基于路径向量路由选择，通过 ISP 边界的路由器加上一定的策略，选择过滤路由，把 RIP、OSPF、BGP 等的路由发送到对方，处理各 AS 之间的路由传递。Internet 是 BGP 处理多个 ISP 间路由的实例。BGP 的出现，引起了 Internet 的重大变革，它把多个 ISP 有机连接起来，真正成为全球范围内的网络。

1）BGP 网络结构

图 3.33 给出了一个 BGP 网络的组成。作为一种外部（边界）网关协议，BGP 主要运行在每个 AS 的边界路由器间。在每个 AS 内部，可以运行 OSPF 或 RIP。运行 BGP 的路由器称为 BGP 说话者（BGP speaker）。BGP 在一对邻接 BGP 说话者之间交换路由信息。这一对邻接的 BGP 称为 BGP 邻居（BGP neighbor），BGP 邻居分为如下两种类型。

- IBGP（内部 BGP 邻居）：位于同一 AS 中的一对 BGP 邻居；
- EBGP（外部 BGP 邻居）：位于不同 AS 中的一对 BGP 邻居。

显然，一个 BGP 网络主要由一些 AS 和一些 BGP 说话者组成，并且通过 BGP 邻居交换路由信息。

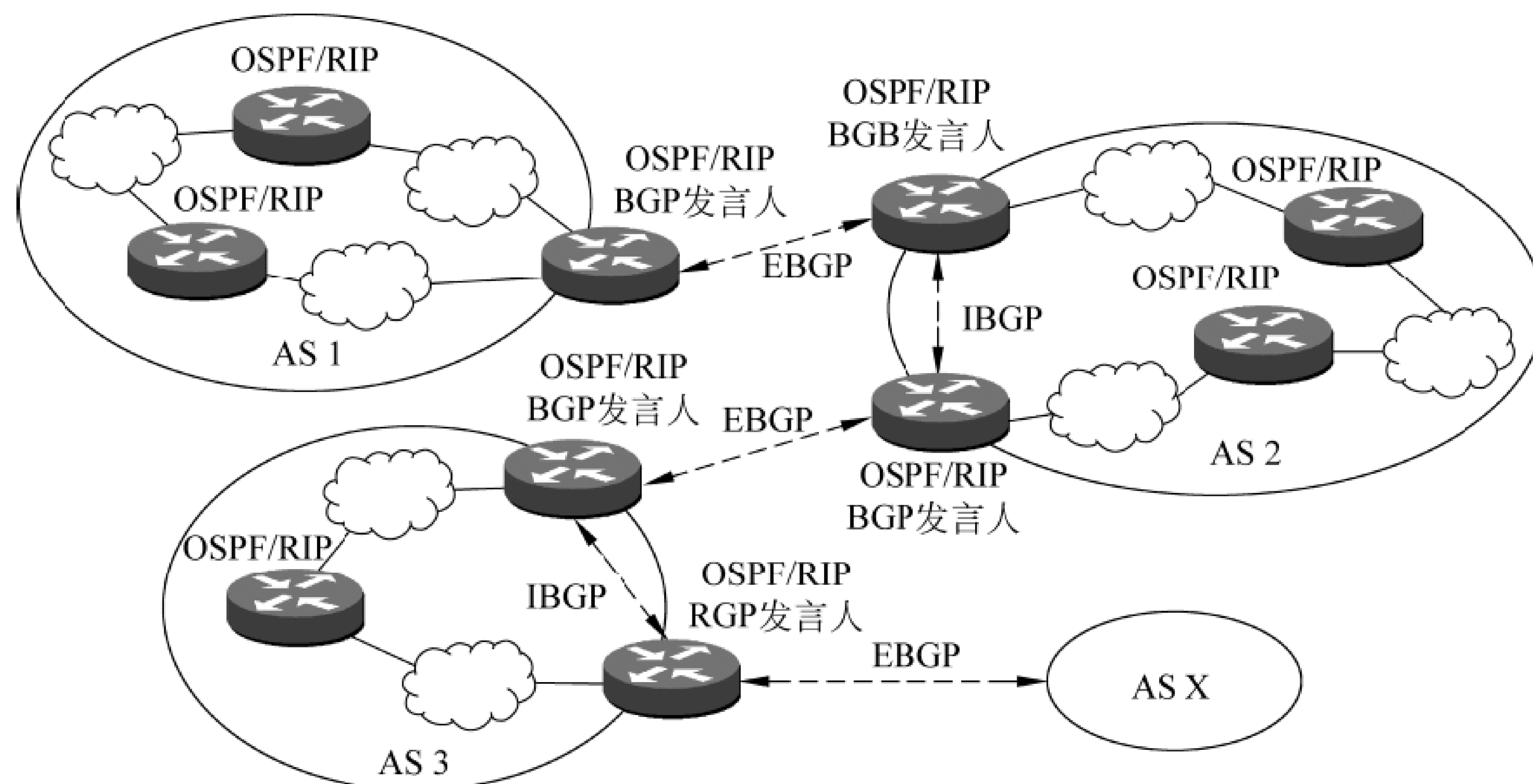


图 3.33　BGP 网络的组成

2）流量类型和 AS 类型

BGP 定义了两种类型的流量：

- 本地流量——在 AS 中发出、在 AS 中终止的流量。
- 传输流量——其他流量都是传输流量。

BGP 的一个目标就是最小化传输流量的总量。

BGP 定义了三种 AS：

- Sub AS——只与另一个 AS 连接，并只承载本地流量。
- 多穴 AS——与一个或两个 AS 连接，但被配置成不转发传输流量。
- 传输 AS——与一个或两个 AS 连接，并被配置成承载本地流量和传输流量。

BGP 在处理路由时，使用 AS 号和 AS 路径：

- AS 号——唯一标识一个 AS 的一个 16b 串。
- AS 路径——描述通过网络路由的 AS 号列表。

3）BGP 路由策略

BGP 是外部网关协议，实现 AS 之间的路由。其路由策略的设置，一般要考虑政治、经济以及安全等多方面的因素。按照到达的目的地，可以将 BGP 的路由策略分为三类。

（1）第一类策略：控制从本 AS 到其他 AS 的路径。例如，制定策略限制本 AS 发出的数据不能经过某些中间自治系统。如某 AS1 中的网络通过 AS2 和 AS3 都可以到达 AS4，但从 AS2 到达 AS4 会经过从安全或商业等角度考虑有问题的 AS5，尽管从 AS2 到达 AS4 是一条最短路径，管理人员还是要选择走 AS3。

（2）第二类策略：控制本 AS 是否为某相邻的 AS 传递过境数据。

（3）第三类策略：实现 AS 内部的协调。

4）BGP 报文类型

所有 BGP 报文都包含了一个标准的报文头，报文头规定了 BGP 报文的类型。有效的 BGP 报文有：

- OPEN（打开）报文。
- KEEPALIVE（保活）报文。
- UPDATE（更新）报文。
- NOTIFICATION（错误条件通知）报文。

（1）OPEN（打开）报文。

一旦在两个对等的结点之间建立了连接，每个路由器就发送一个 OPEN 报文给邻居，请求建立邻接关系。一个 OPEN 报文由一个 KEEPALIVE 报文确认。

OPEN 报文中包含：

- 版本，1b；
- 本 AS 号，2b；
- 保持时间（保持计数器的建议值），2b，定义一方从另一方收到保活（对 OPEN 的应答）或更新报文之前所经过的最大秒数；
- 发端 BGP 路由器标识符，4b；
- 其他。

（2）KEEPALIVE（保活）报文。

运行 BGP 协议的各路由器（在 BGP 中称对等路由器）之间定期地相互交换保活信息，用来通报自己处于 BGP 工作状态，维护 BGP 连接。如果在保持计数器规定的时间内，发送路由器没有收到对等路由器的保活报文，则认为出现了一个错误，即向对等结点发送一个错误通知报文 NOTIFICATION 并关闭连接。

（3）UPDATE（更新）报文。

BGP不定期地刷新整个BGP路由表。刷新使用UPDATE（更新）报文进行。一个UPDATE用来在对等BGP间传输路由信息：公告一个可行的路由，或者撤销那些不可行的路由。其报文中包含如下一些内容：

- 撤销的所有路由。
- 路径属性。用来评估一个路由，宣布本报文可达的网络路径。详见有关手册。
- 网络层可达信息（NLRI）。定义本报文真正通知的网络。

（4）NOTIFICATION（错误条件通知）报文。

当一个BGP设备检测到影响与一个对等结点连接的错误条件时，就发送NOTIFICATION（错误条件通知）报文，关闭与对等结点的连接，解除分配给该连接的所有资源，同时将与远程对等结点相关联的路由表项标记为无效，并通知给其他对等结点。

通知报文包括一个错误代码和一个错误子码。BGP提供了如下一些错误代码：

- 消息报文头错误。
- OPEN 消息错误。
- UPDATE 消息错误。
- 保持计数器超时。
- 有限状态机错误。
- 停止。

3.4.5 路由器配置

不同型号的路由器进行配置的方法不同。下面仅介绍一些基本方法。

1. 路由器的端口

路由器有各种不同的连接对象。对于不同的连接对象，有不同的配置方法。常用端口有如表3.9所示的几种。

表3.9 路由器常用端口类型

端口类型	名　称	标　准
异步串口	async	EIA/TIA RS-232
同步串口	serial	V.24、V.35、EIA/TIA-499、X.21、EIA-530
以太网口	Ethernet	IEEE 802、3RFC894
快速以太网口	FastEthernet	IEEE 802、3RFC894

2. 路由器命令模式

一般的路由器是在命令方式下进行配置和使用的。为了满足不同的使用和使用的安全，路由器提供了不同的命令模式，包括用户模式（user mode）、特权模式（privileged mode）、全局配置模式（configuration mode）等。其中，全局配置模式又包括了一些子配置模式。如图3.34所示为Cisco路由器中几种常用命令模式的状态（提示符）以及相互转换方式。

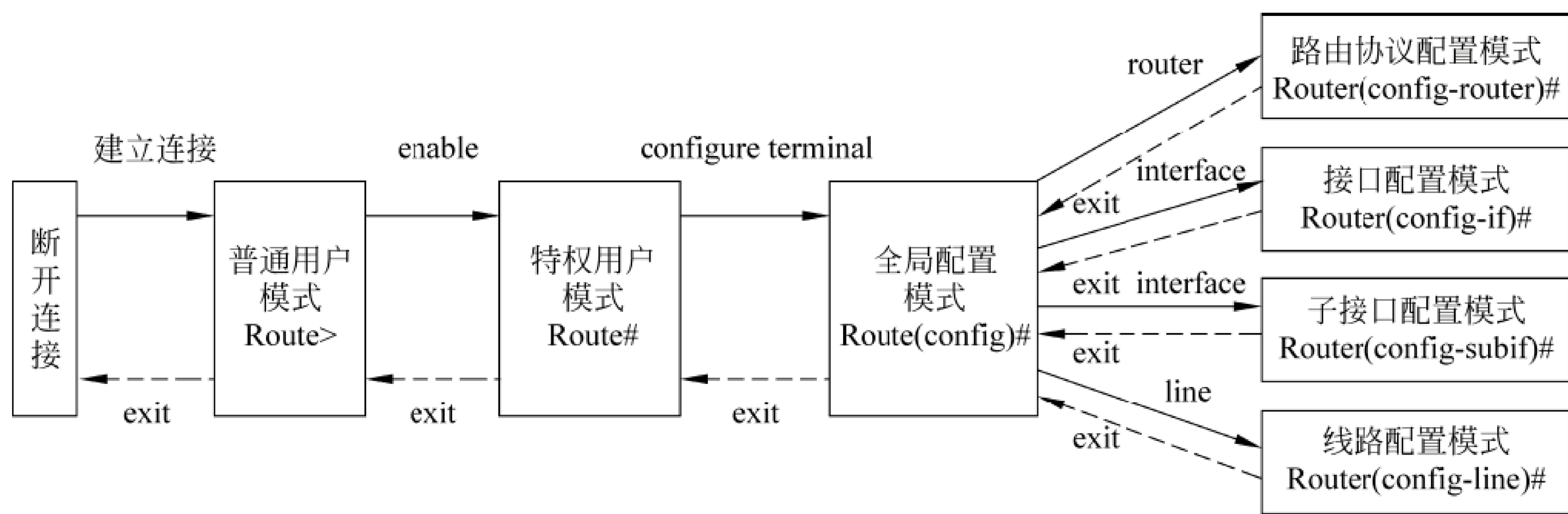


图 3.34　Cisco 路由器中几种常用命令模式的状态（提示符）以及相互转换方式

下面进一步介绍各种模式的用法。

1）普通用户模式

普通用户登录路由器后即处于普通用户模式。这时的提示符为：>。在该模式下，用户只能查看一些路由器当前的使用状态，例如：

```
router>show interface（查看端口信息）
router>show ip route（查看路由表信息）
router>show process cpu（查看路由器当前的 CPU 使用率）
```

在用户模式下无法做进一步的配置。若要再配置，必须转入特权模式。

2）特权用户模式

在普通用户模式下，输入命令：

```
router>enable
```

再输入相应的口令。如果口令正确，就进入了特权模式。这时，提示符变为：#。

注意：这个 enable 口令是进入修改路由器配置的通行证，一定要保存好。

在特权模式下，用户可以使用更多的命令，查看更多的信息，例如：

```
router#show config（查看配置文件内容）
router#debug ip rip（跟踪 RIP 的路由信息交换）
```

3）全局配置模式

在特权模式下输入命令：

```
router#config terminal
```

提示符变为

```
router(config)#
```

即进入了全局配置模式。在此模式下，根据不同的用途，输入相应的命令，进入相应的子配置模式，就可以进行配置了。

3.5　IP 的网络接口

TCP/IP 是面向网络互联的协议栈。在 IP 层解决了主机之间的数据传输之后，需要进一步解决这些分组如何在具体的网络中传输的问题。在 TCP/IP 体系结构中称为网络接口层。

如前所述，TCP/IP 网络体系的分层是人们在其模块结构之上进行的。因此把哪些模块当作网络接口层，有不同的解释。笔者认为作为 TCP/IP 体系与物理网络的接口，应当解决如下问题：

（1）IP 分组如何再被封装成数据链路层的帧。目前广为应用的有 PPP 协议和 PPPoE 协议。这些协议多作为用户接入 Internet 服务商的技术使用。本书将它们放在第 6 章介绍。

（2）IP 地址如何转换为具体网络中的 MAC 地址。这个职责由 TCP/IP 协议栈中的 ARP/RARP 承担。本节主要介绍这个内容。

3.5.1　IP 地址解析协议

IP 地址解析协议（Address Resolution Protocol，ARP）是根据 IP 地址获取物理地址的一种 TCP/IP 协议。

1. 地址解析的概念

IP 地址也称为高级协议地址，是从网络互联的角度对网络、主机和路由器所做的编号，是由软件进行维护的软地址。而每台主机又是在具体的网络中工作的，在那里使用的是另一种地址——物理地址，例如主机采用的是 MAC 地址——每一个网卡的卡号，是由硬件管理的硬地址。

物理网络无法直接根据软地址定位一台主机。为此，要想通过一个物理网进行帧的传送，必须含有目的地的硬件地址（如以太网地址）。将一台计算机的 IP 地址翻译成等价的硬件地址的过程称为地址解析或称地址映射。

2. 地址解析技术

地址解析是通过软件实现的。地址解析软件要根据使用的协议和硬件编址方案来进行地址解析。对于不同的物理网络，由于协议和编址方案不同，解析方法也不相同。例如，将 IP 地址解析为以太网地址与解析为 ATM 网地址的方法是不相同的。

一般说来，大体上有三种地址解析方法。

（1）查表（table lookup）方法：将地址绑定信息存放在高速缓冲存储器内的一张表中，当要进行地址解析时，可以查表找到所需的结果。这种方法常用于 WAN。

（2）相似形式计算（close-form computation）：网络中主机的 IP 地址分配通过对硬件地址的简单逻辑运算和算术运算得到，因而在 IP 地址与物理地址之间存在一种函数关系，可以直接运算求出。这种方法常用于可配置的网络。

（3）报文交换（message exchange）法：前两种方法是集中式地址解析，而报文交换是

分布式地址解析方法，即当一台机器要解析同一网络中另一台计算机的 IP 地址时，先通过网络发送一个请求报文——请求对指定 IP 地址的解析，之后收到一个应答——回答对应的硬件地址。这种方法常用于静态编址的 LAN。

那么，请求报文如何发送呢？通常有两种方法：一是在网络中设立一台或几台服务器，专门用来回答地址解析的请求；二是向全网广播，由各台计算机自己解析自己的 IP 地址。

3. ARP 缓存及其超时设置

ARP 缓存是个用来储存 IP 地址和 MAC 地址的缓冲区，其本质就是一个 IP 地址到 MAC 地址的对应表，表中每一个条目分别记录了网络上其他主机的 IP 地址和对应的 MAC 地址。每一个以太网或令牌环网络适配器都有自己单独的表。当地址解析协议被询问一个已知 IP 地址结点的 MAC 地址时，先在 ARP 缓存中查看，若存在，就直接返回与之对应的 MAC 地址；若不存在，才发送 ARP 请求向局域网查询。

为使广播量最小，ARP 维护 IP 地址到 MAC 地址映射的缓存以便将来使用。ARP 缓存可以包含动态和静态项目。动态项目随时间推移自动添加和删除。每个动态 ARP 缓存项的潜在生命周期是 10 分钟。新加到缓存中的项目带有时间戳，如果某个项目添加后 2 分钟内没有再使用，则此项目过期并从 ARP 缓存中删除；如果某个项目已在使用，则又收到 2 分钟的生命周期；如果某个项目始终在使用，则会另外收到 2 分钟的生命周期，一直到 10 分钟的最长生命周期。静态项目一直保留在缓存中，直到重新启动计算机为止。

4. ARP 分组

为了使所有的计算机共同认可地址解析消息的精确格式和含义，TCP/IP 的地址解析协议 ARP 定义了两种基本的消息：ARP 请求消息（一个请求包含一个 IP 地址和对相应硬件的请求，格式如图 3.35 所示）和 ARP 应答消息（一个应答消息既包含发来的 IP 地址，也包含相应的硬件地址）。ARP 规定：所有 ARP 请求消息都直接封装在 LAN 帧中，广播给网上的所有计算机，每台计算机收到这个请求消息后都要检测其中的 IP 地址；与 IP 地址匹配的计算机即发出一个应答消息，而其他计算机则丢弃收到的请求，不发出任何应答。

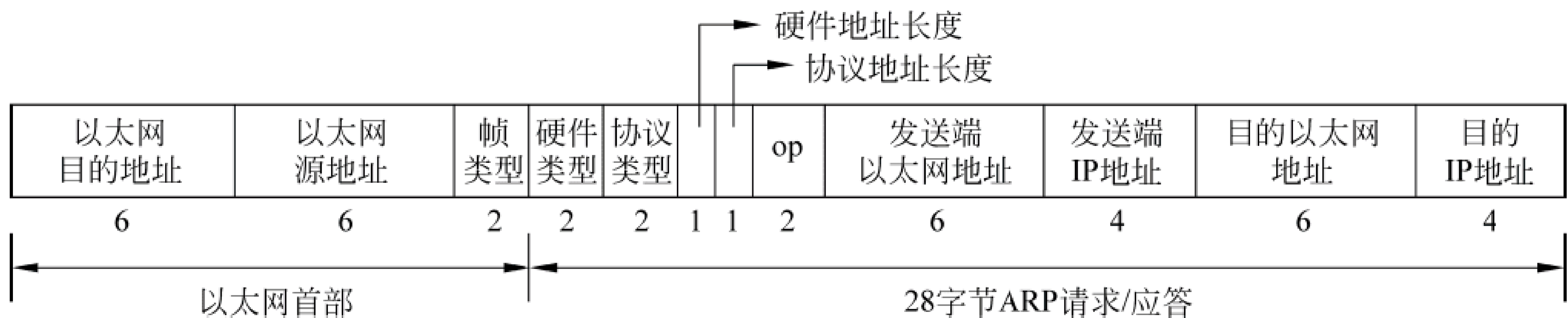


图 3.35　用于以太网的 ARP 分组格式

说明：

（1）硬件类型指明了发送方想知道的硬件接口类型，以太网的值为 1。

（2）协议类型指明了发送方提供的高层协议类型，IP 为 0800（十六进制）。通过对一个帧中协议类型的判断，一台计算机可以知道该帧中是否含有 ARP 报文。例如当一个以太网帧携带有 ARP 报文时，类型字段中就包含十六进制数 0x806。

（3）硬件地址长度和协议长度指明了硬件地址和高层协议地址的长度。它们会因硬件和协议而不同。这样，ARP 报文就可以在任意硬件和任意协议的网络中使用。

（4）操作类型用来表示这个报文的类型，ARP 请求为 1，ARP 响应为 2，RARP 请求为 3，RARP 响应为 4。

5. 同一个网络内部的地址解析过程举例

假设：

主机 A 的 IP 地址为 192.168.1.1，MAC 地址为 0A-11-22-33-44-01；

主机 B 的 IP 地址为 192.168.1.2，MAC 地址为 0A-11-22-33-44-02。

当主机 A 要与主机 B 通信时，地址解析协议可以将主机 B 的 IP 地址（192.168.1.2）解析成主机 B 的 MAC 地址，以下为工作流程：

（1）根据主机 A 上的路由表内容，IP 确定用于访问主机 B 的转发 IP 地址是 192.168.1.2。然后 A 主机在自己的本地 ARP 缓存中检查主机 B 的匹配 MAC 地址。

（2）如果主机 A 在 ARP 缓存中没有找到映射，它将询问 192.168.1.2 的硬件地址，从而将 ARP 请求帧广播到本地网络上的所有主机。源主机 A 的 IP 地址和 MAC 地址都包括在 ARP 请求中。本地网络上的每台主机都接收到 ARP 请求并且检查是否与自己的 IP 地址匹配。如果主机发现请求的 IP 地址与自己的 IP 地址不匹配，它将丢弃 ARP 请求。

（3）主机 B 确定 ARP 请求中的 IP 地址与自己的 IP 地址匹配，则将主机 A 的 IP 地址和 MAC 地址映射添加到本地 ARP 缓存中。

（4）主机 B 将包含其 MAC 地址的 ARP 回复消息直接发送回主机 A。

（5）当主机 A 收到从主机 B 发来的 ARP 回复消息时，会用主机 B 的 IP 和 MAC 地址映射更新 ARP 缓存。本机缓存是有生存期的，生存期结束后，将再次重复上面的过程。主机 B 的 MAC 地址一旦确定，主机 A 就能向主机 B 发送 IP 通信了。

6. ARP 代理与不同网络之间的地址解析过程

地址解析是同一个网络内部的局部过程，即一台计算机只能够解析位于同一网络中的另一台计算机地址。如果 ARP 请求是从一个网络的主机发往另一个网络上的主机，那么连接这两个网络的路由器就可以回答该请求，这个过程称作委托 ARP 或 ARP 代理（Proxy ARP）。这样可以欺骗发起 ARP 请求的发送端，使它误以为路由器就是目的主机，而事实上目的主机是在路由器的“另一边”。路由器的功能相当于目的主机的代理，把分组从其他主机转发给它。

在图 3.36 中，主机 A 上的一个应用程序要传输一条报文到主机 F 上，由于 A 与 F 不在同一个网络上，因此 A 上的软件无法解析 F 的地址，于是这个报文的传输要经过如下过程：

（1）主机 A 上的软件首先确定要将报文传输到 F 必须经过路由器 R_1，于是解析位于同一网络中路由器 R_1 的地址，将报文传送到 R_1；

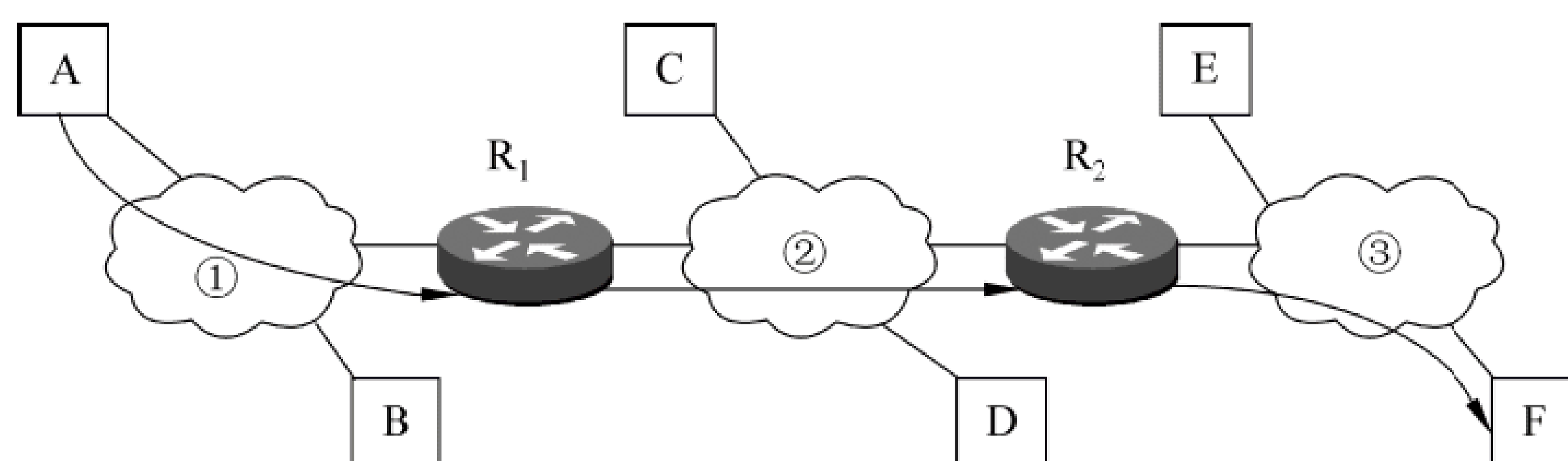


图 3.36　地址解析实例

（2）路由器 R_1 上的软件确定要将报文传输到 F 必须经过路由器 R_2，于是解析位于同一网络中路由器 R_2 的地址，将报文传送到 R_2；

（3）路由器 R_2 上的软件确定 F 就在同一网络上，于是解析位于同一网络中主机 F 的地址，将报文传送到 F。

7. 反向地址解析协议 RARP

IP 层中还包含一个反向地址解析协议 RARP，用于规定硬件地址到等价的 IP 地址的翻译过程。反向地址转换协议（RARP）是局域网的物理机器从网关服务器的 ARP 表或者缓存中根据 MAC 地址请求 IP 地址的协议，其功能与地址解析协议相反。与 ARP 相比，RARP 的工作流程也相反。首先是查询主机向网络送出一个 RARP Request 广播封包，向别的主机查询自己的 IP 地址。这时候网络上的 RARP 服务器就会将发送端的 IP 地址用 RARP Reply 封包回应给查询者，这样查询主机就获得自己的 IP 地址了。

需要说明的是，TCP/IP 的分层是不太严格的，ARP/RARP 可以看作 IP 层的协议，也可以看成是网络接口层的协议。

8. ARP 命令

ARP 命令用于查询本机 ARP 缓存中 IP 地址→MAC 地址的对应关系，添加或删除静态对应关系等。如果在没有参数的情况下使用，ARP 命令将显示帮助信息。

1）命令语法

```
arp[-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr
[IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]
```

2）参数

- -a[InetAddr] [-N IfaceAddr]：显示所有接口的当前 ARP 缓存表。要显示特定 IP 地址的 ARP 缓存项，请使用带有 InetAddr 参数的 arp -a，此处的 InetAddr 代表 IP 地址。如果未指定 InetAddr，则使用第一个适用的接口。要显示特定接口的 ARP 缓存表，请将 -N IfaceAddr 参数与 -a 参数一起使用，此处的 IfaceAddr 代表指派给该接口的 IP 地址。-N 参数区分大小写。
- -g[InetAddr] [-N IfaceAddr]：与 -a 相同。
- -d InetAddr [IfaceAddr]：删除指定的 IP 地址项，此处的 InetAddr 代表 IP 地址。对于指定的接口，要删除表中的某项，请使用 IfaceAddr 参数，此处的 IfaceAddr 代表指派给该接口的 IP 地址。要删除所有项，请使用星号 (*) 通配符代替 InetAddr。

- -s InetAddr EtherAddr [IfaceAddr]：向 ARP 缓存添加可将 IP 地址 InetAddr 解析成物理地址 EtherAddr 的静态项。要向指定接口的表添加静态 ARP 缓存项，请使用 IfaceAddr 参数，此处的 IfaceAddr 代表指派给该接口的 IP 地址。
- /?：在命令提示符下显示帮助。

3）注释

（1）InetAddr 和 IfaceAddr 的 IP 地址用带圆点的十进制记数法表示。

（2）EtherAddr 的物理地址由六个字节组成，这些字节用十六进制记数法表示并且用连字符隔开（比如，00-AA-00-4F-2A-9C）。

（3）通过 -s 参数添加的项属于静态项，它们不会 ARP 缓存超时。如果终止 TCP/IP 协议后再启动，这些项会被删除。要创建永久的静态 ARP 缓存项，请将适当的 arp 命令置于批处理文件中，并使用“任务计划”功能在启动时运行该批处理文件。

4）常见用法

```
arp -a 或 arp -g
```

用于查看缓存中的所有项目。-a 和-g 参数的结果是一样的，多年来-g 一直是 UNIX 平台上用来显示 ARP 缓存中所有项目的选项，而 Windows 用的是 arp -a（-a 可被视为 all，即全部的意思），但它也可以接受比较传统的-g 选项。

```
arp -a Ip
```

如果有多个网卡，那么使用 arp -a 加上接口的 IP 地址，可以只显示与该接口相关的 ARP 缓存项目。

```
arp -s Ip 物理地址
```

将一个 IP 地址与一个物理地址绑定，以防止 IP 地址被盗用。如果不绑定，当一台设备上网时，得到的 IP 地址是由路由器动态分配的。

```
arp -d Ip
```

使用该命令能够人工删除一个静态项目。

3.5.2　邻居发现协议

地址解析协议是 IPv4 中必不可少的协议，但在 IPv6 中将不再存在地址解析协议。在 IPv6 中，地址解析协议的功能将由邻居发现协议（Neighbor Discovery Protocol，NDP）实现，它使用一系列 IPv6 控制信息报文（ICMPv6）来实现相邻结点（同一链路上的结点）的交互管理，并在一个子网中保持网络层地址和数据链路层地址之间的映射。邻居发现协议中定义了 5 种类型的信息：路由器宣告、路由器请求、路由重定向、邻居请求和邻居宣告。与 ARP 相比，NDP 可以实现路由器发现、前缀发现、参数发现、地址自动配置、地址解析（代替 ARP 和 RARP）、下一跳确定、邻居不可达检测、重复地址检测、重定向等更多功能。

NDP 与 ARP 有如下不同：

（1）IPv4 中地址解析协议是独立的协议，负责 IP 地址到 MAC 地址的转换，对不同的数据链路层协议要定义不同的地址解析协议。IPv6 中 NDP 包含了 ARP 的功能，且运行于 Internet 控制信息协议 ICMPv6 上，更具有一般性，包括更多的内容，而且适用于各种数据链路层协议。

（2）地址解析协议以及 ICMPv4 路由器发现和 ICMPv4 重定向报文基于广播，而 NDP 的邻居发现报文基于高效的组播和单播。

实验 6　使用 TCP/UDP 吞吐量测试工具 TTCP

测试网络性能吞吐量可以采用 FTP 方法，即在测试路径的两端分别运行 FTP 服务器和客户端软件，传送一个很大的文件，记录传送完成之后软件显示的速率统计。这种测试方法有个很大的问题，就是测试结果受到测试机器的磁盘读写速度的影响，使用也不方便。而 TTCP（Test TCP）直接可以从内存生成要传送的数据，通过网络传送接收后无须写到磁盘，直接丢弃。

TTCP 时间，就是在两个系统中间利用 UDP 和 TCP 协议传输和接收数据的时间。TTCP 既可以用 TCP 也可以用 UDP，而通常的测量方法不允许在远程 UDP 传输的终端进行测量。这也是 TTCP 相比其他测试工具所具备的优点。

一、TTCP 安装

Linux 下的安装文件有两个版本：一个是基于 Java 的；另一个就是基于 C 的。

下载一个 rpm 包和 **ttcp.c**，安装过程如下：

```
[root@localhost root]# rpm -ihv /home/neo/fastweb/ttcp-1.12-7.i386.rpm
Preparing...                ###########################################[100%]
1:ttcp                  ########################################### [100%]
[root@localhost root]# rpm -qil ttcp
Name        : ttcp                        Relocations: (not relocateable)
[...]
```

安装完成后，包含以下文件：

（1）主文件路径

```
/usr/bin/ttcp
```

（2）说明文档路径

```
/usr/share/doc/ttcp-1.12
/usr/share/doc/ttcp-1.12/README
/usr/share/man/man1/ttcp.1.gz
```

编译 ttcp.c

```
[root@dido root]# gcc -O3 -o ttcp ttcp.c
ttcp.c:539: warning: static declaration for 'gettimeofday' follows non-static
```

二、启动 TTCP

1）启动 TTCP 发送端进程

```
ttcp  -t  [-u]  [-s]  [-p port]  [-l buflen]  [-b size]  [-n numbufs] [-A align] [-O offset]
[-f format] [-D] [-v] host [<in]
```

2）启动 TTCP 接收端进程

```
ttcp  -r [-u] [-s] [-p port] [-l buflen] [-b size]  [-A align]  [-O offset]  [-f format]
[-B] [-T] [-v] [>out]
```

三、参数选项

-t：指定传送模式。

-r：指定接收模式。

-u：指定使用 UDP（默认使用 TCP）来发送数据。

-s：发送一个字符串作为传送的包的有效负载。不使用-s，则默认情况是传送发送方的终端窗口（stdin）的数据，以及将接收到的数据显示到接收方的终端窗口。

-l：指定缓冲区长度为 buflen（默认是 8192B）。对于 UDP，是显示每个报文的数据字节，即系统限制最大的 UDP 报文长度。这个限制能被-b 选项来改变。

-b：设置接口缓冲区长度 size。这个变量影响 UDP 包的最大长度。在有些系统上不能设置这个变量（例如，4.2BSD）。

-n：设置要传送的用户数据的块数量 numbufs（默认值为 2048）。

-p：指定发送或者被侦听的端口号 port（默认值是 2000）。发送方端口号与接收方端口号必须相同。

-D：禁用 TCP 的数据缓冲区，强迫立即传送 TTCP 发送方中的数据。只用于 TTCP 上下文中，在有些系统上不能设置这个变量（例如，4.2BSD）。

-B：接收数据时完全使用了大小被指定为-l 的块。

-A：设置排列缓冲区的初始地址为 align（默认值为 16 384）。

-T：测量缓存性能的数据。

-v：详细——打印更多的统计表。

-d：调试——设置 SO_DEBUG 接口选项。

四、测试过程

运行 TTCP 工具需要设置一台主机为 TTCP 接收方，然后设置一台主机为 TTCP 发送方，传输端发送 TCP 或者 UDP 信息的指定的编号到接收端。一旦发送方启动，它就会尽可能快速地向接收方发送指定数量的数据。因此，做一个测试，至少要两个主机：第一个作为传送方，第二个作为接收方。

注意：测试网络之前，务必先测试一下所用的测试机器（如用交叉线将两台机器直连起来测试）一下，以保证测试涉及的两个设备之间的 IP 连通性。

(1)接收端的终端窗口(stdout)通过-r 选项、-v 选项和-s 选项接收发送方终端窗口(stdin)数据，本例中默认的侦听端口为 5001。

```
[root@nefertiti root]# ttcp -r -v -s
ttcp-r: buflen=8192, nbuf=2048, align=16384/0, port=5001  tcp
ttcp-r: socket
```

(2) 发送方通过-t 选项，将数据放入接收方的清单并且通过网络管道完成接收功能，接收方的 IP 为 192.168.1.2。

```
[root@pippo root]# ttcp -t -v -s 192.168.1.2
ttcp-r: accept from 192.168.1.5
ttcp-t: 16777216 bytes in 408.85 real seconds = 40.07 KB/sec +++
ttcp-t: 16777216 bytes in 0.00 CPU seconds = 1638400000.00 KB/cpu sec
ttcp-t: 2048 I/O calls, msec/call = 204.42, calls/sec = 5.01
ttcp-t: 0.0user 0.0sys 6:48real 0% 0i+0d 0maxrss 0+2pf 0+0csw
ttcp-t: buffer address 0x8050000
```

五、一个例子 "network pipe"

```
[root@pippo root]# ttcp -rvs | ttcp -tvs 192.168.1.5
ttcp-r: socket
ttcp-t: buflen=8192, nbuf=2048, align=16384/0, port=5001  tcp  ->
192.168.1.5
ttcp-t: socket
ttcp-t: connect
```

在这个例子中，发送方通过端口 5001 将数据发送到 IP 为 192.168.1.5 的接收端。

实验 7　利用 ping 命令测试网络的连通性

一、实验内容

利用 ping 命令测试 IP 网络的连通性。

二、实验准备

获得要测试主机的 IP 地址。

三、ping 命令介绍

1. 命令格式

```
ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s
count] [-j computer-list] | [-k computer-list] [-w timeout] destination-list
```

2. 参数说明

-t：使当前主机不断向目的主机发送数据，直到按 Ctrl+C 组合键中断。

-a：将地址解析为域名。

-n count 发送 count 指定的 ECHO 数据包数，默认值为 4。

-l length 发送包含由 length 指定的数据量的 ECHO 数据包。默认为 32B；最大值是 65，527。

-f 在数据包中发送“不要分段”标志。数据包就不会被路由上的网关分段。

-i TTL：用 TTL 指定“生存时间”字段的值。

-v TOS：用 TOS 指定服务类型。

-r count 在“记录路由”字段中记录传出和返回数据包的路由。最少 1 台，最多 9 台计算机。

-s count：用 count 指定跳点数的时间戳。

-j computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源），IP 允许的最大数量为 9。

-k computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源），IP 允许的最大数量为 9。

-w timeout 指定超时间隔，单位为毫秒，默认值为 1000。

destination-list 指定要 ping 的远程计算机。

四、实验参考步骤

（1）运行“开始”→“运行”命令，弹出如图 3.37 所示的“运行”对话框。

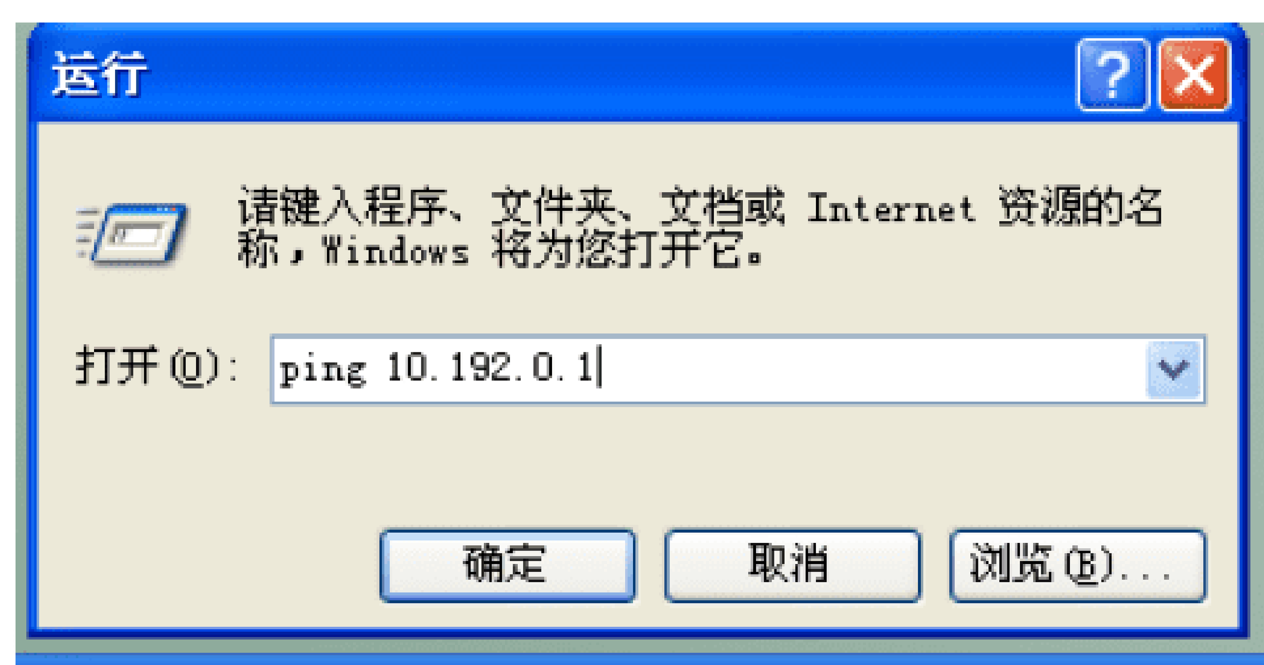


图 3.37　在“运行”对话框内输入 ping 命令

（2）在命令行中输入 ping 命令，格式为

```
ping <某主机 IP 地址>
```

例如，输入网关 IP 地址，单击“确定”按钮。如果能得到回应，表示本机到这台主机（如网关）连通。如图 3.38 所示为对上述命令的回应情况。

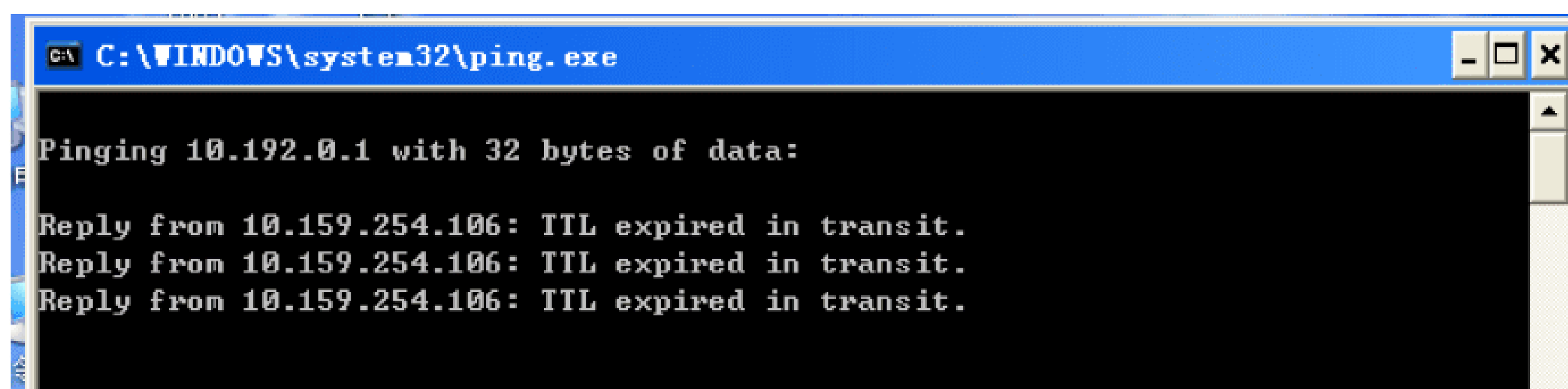


图 3.38　测试结果显示

五、分析与讨论

（1）分析 ping 命令的工作原理。

（2）对 ping 命令的其他用法进行测试。

（3）ping 命令能对没有连接到 Internet 的局域网进行连通性测试吗？

实验 8　路由器的端口配置

一、实验内容

（1）路由器的端口配置。

（2）路由器端口配置后的连通性测试。

二、实验准备

（1）本次实验使用的网络接线图。参考的实验用网络接线图如图 3.39 所示。

（2）设备配置。

- Cisco 路由器两台；
- 交换机两台；
- 实验用计算机 4 台以上；
- 网线若干条。

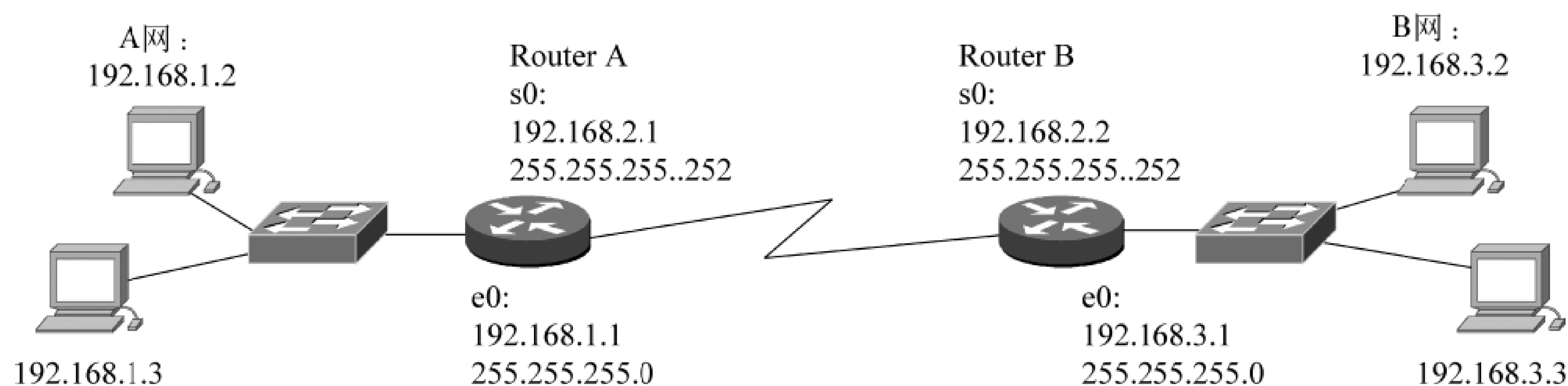


图 3.39　参考的实验用网络接线图

三、实验参考步骤

1. 网络连接

按照实验线路图连接网络，特别注意路由器的连接。

- 路由器的串口（s0）之间用广域网线互连，其中，Router A 连接 DCE 端，Router B 连接 DTE 端。
- 路由器的以太网口（e0）与交换机连接。

2. Router A 的端口配置

端口配置的目的是将端口的物理地址与分配的 IP 地址绑定。配置方法如下：

（1）路由器加电→进入普通用户模式→进入特权（超级）用户模式 Router A#→进入全局配置模式：

```
Router A(config)#
```

（2）配置 Router A 的 e0 端口：

```
Router A(config)#interface e0                          //进入 e0 的端口配置模式
Router A(config-if)#ip address 192.168.1.1 255.255.255.0  //设置 e0 的 IP 地址和子网掩码
Router A(config-if)#no shutdown                        //开启 e0 端口的配置
RouterA#show ip interface e0                           //验证 e0 的 IP 地址已经配置和开启
```

（3）配置 Router A 的 s0 端口：

```
Router A(config)#interface s0                          //进入 s0 的端口配置模式
Router A(config-if)#ip address 192.168.2.1 255.255.255.252  //设置 e0 的 IP 地址和子网掩码
Router A(config-if)#clock rate 64000                   //设置时钟频率(DCE 端要求)
Router A(config-if)#no shutdown                        //开启 s0 端口
```

3. Router B 的端口配置

方法同 Router B 的端口配置，但不需再设置时钟频率。

4. 连通性测试

（1）在 A 网的一台计算机上，用 ping 命令测试下面的连通性：

```
ping 192.168.2.1
ping 192.168.1.1
ping 192.168.2.2
ping 192.168.3.1
ping 192.168.3.2
```

（2）在 Router A 上，用 ping 命令测试下面的连通性：

```
ping 192.168.1.2
ping 192.168.1.1
ping 192.168.2.2
ping 192.168.3.1
ping 192.168.3.2
```

说明：在路由器中，ping 其他设备时显示界面与在计算机上的 ping 界面不同，如果 ping 结果中显示 5 个叹号“!!!!!”，就说明可以连通；如果显示“……”，则说明不通。

四、分析与讨论

（1）为什么在 A 网的一台计算机上，可以 ping 通 Router A 的 E0 端口和 Router A 的 S0 端口，但不能 ping 通 Router B 和 B 网中的计算机？

（2）为什么在 Router A 上，可以 ping 通 A 网中的计算机和 Router B，但不能 ping 通 Router B 的 E0 端口和 B 网中的计算机？

实验 9　静态路由配置

一、实验内容

（1）路由器的静态路由配置。
（2）静态路由配置后的网络连通性测试。

二、实验准备

（1）本次实验使用的网络接线图。参考的实验用网络接线图如图 3.17 所示。
（2）网络已经连接，路由器的端口已经配置。
（3）路由协议没有配置，或已经清除了已有的路由配置。

三、实验参考步骤

1. 在 Router A 上进行静态路由配置
（1）进入全局配置模式：

```
Router A(config)#
```

（2）进行静态路由配置，命令如下：

```
Router A(config)#ip route 192.168.3.0 255.255.255.0     192.168.2.2
! 目标网段地址为 192.168.3.0，子网掩码为 255.255.255.0，下一跳经过的端口 IP 地址为 192.168.2.2
```

按回车键后生效。
（3）连通性测试：
在 A 网的一台计算机上用 ping 命令测试下面的连通性：

```
ping 192.168.2.1
ping 192.168.1.1
ping 192.168.2.2
ping 192.168.3.1
ping 192.168.3.2
```

在 Router A 上用 ping 命令测试下面的连通性：

```
ping 192.168.1.2
ping 192.168.1.1
ping 192.168.2.2
ping 192.168.3.1
ping 192.168.3.2
```

在 B 网的一台计算机上用 ping 命令测试下面的连通性：

```
ping 192.168.2.2
ping 192.168.3.1
```

```
ping 192.168.2.1
ping 192.168.1.1
ping 192.168.2.2
```

在 Router B 上用 ping 命令测试下面的连通性：

```
ping 192.168.3.2
ping 192.168.3.1
ping 192.168.2.1
ping 192.168.1.1
ping 192.168.1.2
```

2. 在 Router B 上进行静态路由配置

方法同在 Router B 上进行静态路由配置，并进行同样的连通性测试。

3. 删除静态路由

（1）删除 Router A 上的静态路由配置：

```
Router A(config)#no ip route 192.168.3.0 255.255.255.0  192.168.2.2
```

（2）连通性测试。

（3）删除 Router B 上的静态路由配置，并进行同样连通性测试。

四、分析与讨论

（1）对于上述 4 次操作后测试的结果列表进行比较，找出规律。

（2）什么情况下要进行删除静态路由的操作？

实验 10　动态路由配置

一、实验内容

（1）路由器的动态路由配置。

（2）动态路由配置后的网络连通性测试。

二、实验准备

（1）本次实验使用的网络接线图（可以参考图 3.39）。

（2）网络已经连接，路由器的端口已经配置。

（3）路由协议没有配置，或已经清除了已有的路由配置。

三、实验参考步骤

1. RIP 路由配置

（1）配置 RIP 路由

在 Router A 上，进入全局配置模式 Router A(config)#，执行如下命令：

```
Router A(config)#router rip                          //启动 RIP 路由协议
Router A(config-router)#network 192.168.1.0          //声明相邻网络
Router A(config-router)#network 192.168.2. 0         //声明相邻网络
```

在 Router B 上配置 RIP 路由，方法同上。

（2）连通性测试，参照静态路由配置后的测试。

（3）删除 RIP 路由，方法是可以在 Router A 和 Router B 上，分别执行下面的命令：

```
Router A(config)#no router rip
```

2. IGRP 路由配置

（1）配置。

在 Router A 上，进入全局配置模式 Router A(config)#，执行如下命令：

```
Router A(config)#router igrp 100                     //启动 IGRP 路由协议，100 为进程号
Router A(config-router)#network 192.168.1.0          //声明相邻网络
Router A(config-router)#network 192.168.2.0          //声明相邻网络
```

在 Router B 上，进入全局配置模式 Router B(config)#，执行如下命令：

```
Router B(config)#router igrp 100                     //启动 IGRP 路由协议，100 为进程号
Router B(config-router)#network 192.168.2.0          //声明相邻网络
Router B(config-router)#network 192.168.3.0          //声明相邻网络
```

（2）连通性测试，参照静态路由配置后的测试。

（3）删除配置，参照 RIP 的删除。

四、分析与讨论

比较 RIP 与 IGRP 路由协议。

习　题　3

一、选择题

1．传输层的作用不包括下列【　　】。

　A．建立运输站　　　　　　　　B．拆除运输站

　C．把信息组装成包　　　　　　D．负责数据传输

2．Internet的核心协议是【　　】。

　A．X.25　　　　B．TCP/IP　　　　C．ICMP　　　　D．UDP

3．TCP/IP体系结构中的TCP和IP所提供的服务分别为【　　】。

　A．链路层服务和网络层服务　　B．网络层服务和传输层服务

　C．传输层服务和应用层服务　　D．传输层服务和网络层服务

4．下列关于TCP和UDP的说法，正确的是【　　】。

　A．两者都是面向无连接的　　　B．两者都是面向连接的

C．TCP是面向连接而UDP是无连接的　　D．TCP是无连接而UDP是面向连接的

5．下列4个选项中，是合法IP地址的是【　　】。

A．202.96.266.2　B．10.1. .8　C．192.168.1.A　D．192.168.1.1

6．按IP地址分类，地址168.201.64.2属于【　　】类地址。

A．A　B．C　C．B　D．D

7．下列【　　】地址可分配给主机作为C类IP地址使用。

A．127.0.0.1　B．192.12.25.255　C．202.96.96.0　D．162.3.5.1

8．如果一个C类网络用掩码255.255.255.192划分子网，那么会产生【　　】个可用的子网。

A．16　B．6　C．2　D．4

9．C类IP地址是指【　　】。

A．每个地址的长度为48位　　B．可以表示16 382个网络

C．每个C类网络最多可以有254个结点　　D．编址时第一位为0

10．用户数据报协议（User Datagram Protocol，UDP）是【　　】。

A．一种面向连接的协议

B．一种简单的、面向数据报的传输层协议

C．主要用在要求数据发送确认或者通常需要传输大量数据的应用程序中

D．一种可靠的传输方式

二、简答题

1．某IP地址的十六进制表示为：C22F1588，请将其转换成点分十进制表示。

2．IP地址的作用是什么？IPv4和IPv6的IP地址有什么不同？

3．什么是子网掩码？C类地址的默认子网掩码是多少？

4．比较你所知道的几种路由协议的特点。

第 4 章　Internet 应用

计算机网络应用是一系列网络应用的总称。TCP/IP 协议栈中没有定义应用层的实现。这反而给应用层提供了巨大的灵活性和不断扩充的条件。目前，已经对 Internet 开发出多种应用。

每一种网络应用都有自己的应用层协议，用来规定这种网络应用所应当遵守的通信规则。表 4.1 为几种主要 Internet 应用所需要的 TCP/UDP 支持。简单地说，TCP 服务就是面向连接的服务，UDP 服务就是数据报服务。

表 4.1　几种主要 Internet 应用所需要的 TCP/UDP 支持

Internet 应用	应用层协议	TCP/UDP 支持
文件传输	FTP（File Transfer Protocol）	TCP
超文本传输	HTTP（HyperText Trasfer Protocol）	TCP
电子邮件	SMTP（Simple Mail Transfer Protocal）	TCP
远程终端访问	TELNET（Teletype Network）	TCP
IP 电话	专用协议	通常 UDP
流媒体	专用协议	UDP/TCP

4.1　域名服务系统

随着 TCP/IP 成为网络的实际标准，IP 地址的记忆问题便浮现出来，成为了 Internet 进一步推广的瓶颈。人们迫切希望能用容易记忆的名字串代替 IP 地址，于是开发了域名系统（Domain Name System，DNS）来实现域名管理及其与 IP 地址之间的转换。有了域名系统，为广大 Internet 用户提供了极大的便利。

4.1.1　域名空间

1．域名空间及其结构

DNS 将域名数据分类，并采用分布式与层次式方式进行处理。这个树形结构的域名系统组成了如图 4.1 所示的域名空间。

2．顶级域名

在一个具体的域名中，放在最右面的词称为顶级域名。早期人们使用的顶级域名分为三类：

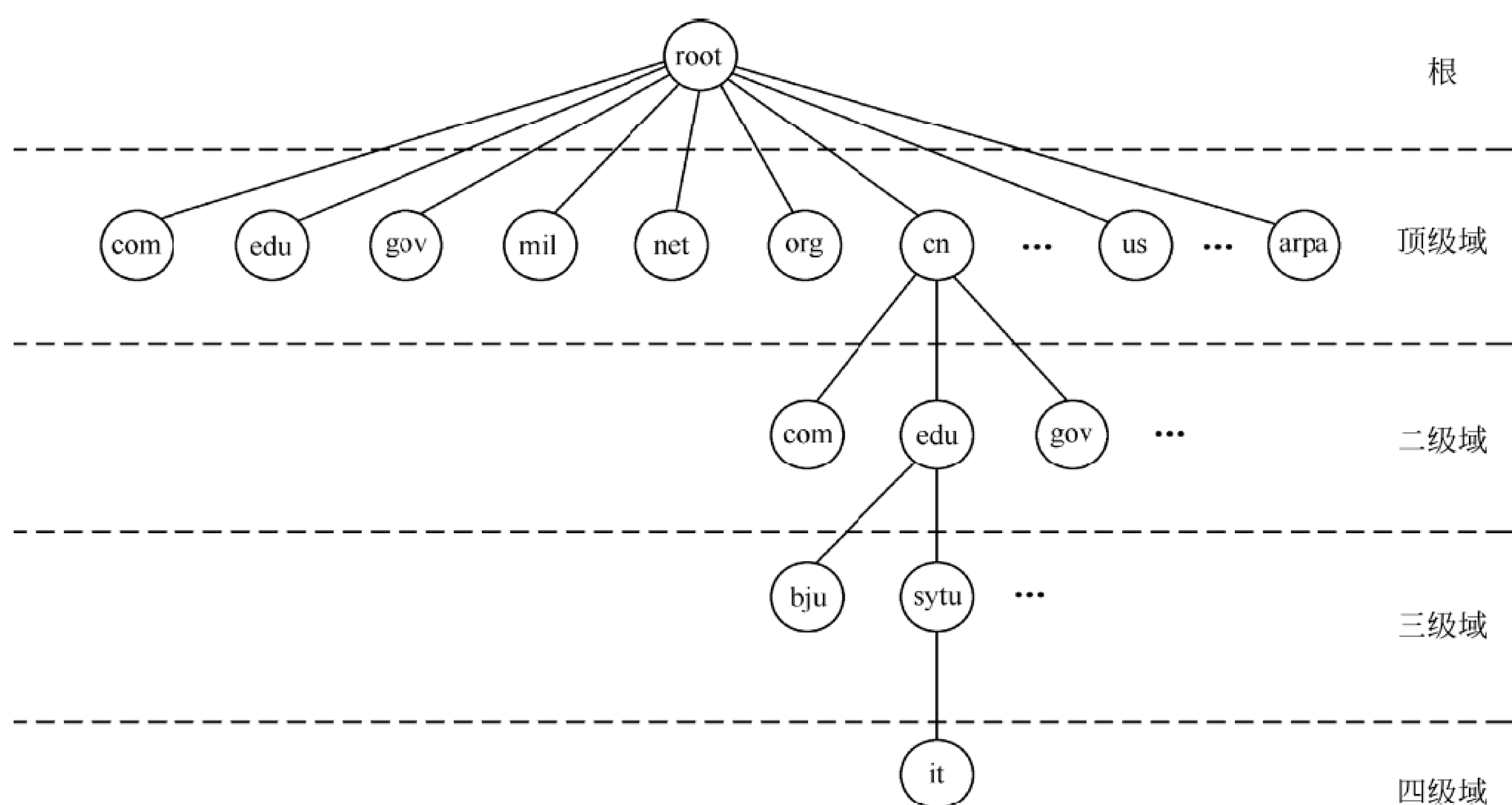


图 4.1　域名空间

（1）国际顶级域名（international Top-level Domain names，iTDs），例如表示工商企业的 .com，表示网络提供商的.net，表示非营利组织的.org 等，如表 4.2 所示。

表 4.2　最常使用的国际顶级域名

域	描　述
com	商业机构（Commercial organization）
edu	教育机构（Education institution）
gov	政府机构（Government agencies）
int	国际组织（International orgnization）
mil	军事机构（Military agencies）
net	网络服务机构（Network support center）
org	非营利机构（Non-profit organization）

（2）国家和地区顶级域名（country code Top-Level Domains，nTLDs），目前 200 多个国家都按照 ISO 3166 国家代码分配了顶级域名，例如中国是 cn，日本是 jp 等，如表 4.3 所示。

（3）新顶级域（New gTLD Overview）如.red 等。

大多数域名争议都发生在 com 的顶级域名下，因为多数公司上网的目的都是为了赢利。为加强域名管理，解决域名资源的紧张，Internet 协会、Internet 分址机构及世界知识产权组织（WIPO）等国际组织经过广泛协商，在原来三个国际通用顶级域名：（com）的基础上，新增加了 7 个国际通用顶级域名：firm（公司企业）、store（销售公司或企业）、Web（突出 WWW 活动的单位）、arts（突出文化、娱乐活动的单位）、rec (突出消遣、娱乐活动的单位)、info(提供信息服务的单位）、nom(个人)，并在世界范围内选择新的注册机构来受理域名注册申请。

表 4.3　主要的国家与地区顶级域名

域名	含　义	域名	含　义	域名	含　义
aq	南极大陆	fr	法国	nl	荷兰
ar	阿根廷	gb	大不列颠（同 uk）	no	挪威
at	奥地利	gr	希腊	nz	新西兰
au	澳大利亚	hk	中国香港地区	pl	波兰
be	比利时	hu	匈牙利	pr	波多黎各
bg	保加利亚	ie	爱尔兰	pt	葡萄牙
br	巴西	il	以色列	se	瑞典
ca	加拿大	in	印度	sg	新加坡
ch	瑞士	is	冰岛	su	（前）苏联
cl	智利	it	意大利	th	泰国
cn	中国	jp	日本	tw	中国台湾地区
de	德国	kr	韩国	uk	英国
dk	丹麦	kw	科威特	us	美国
ec	厄瓜多尔	lt	立陶宛	ve	委内瑞拉
eg	埃及	lu	卢森堡	yu	南斯拉夫
es	西班牙	mx	墨西哥	za	南非
fi	芬兰	my	马来西亚		

4.1.2　域名规则

1．英文域名规则

1）域名的组成

- 26 个英文字母；
- 数字 0～9；
- 英文中的连词符“-”（不得用于开头及结尾处）。

2）域名中字符组合规则

- 在域名中不区分英文字母的大小写；
- 空格及符号，如 ？ /\； ：@ # $ % ^ ～_ = +，. 。 < >等，都不能用在域名中；
- 英文域名命名长度限制介于 2～46 个字符，三级域名长度不得超过 20 个字符；
- 各级域名之间用实点（.）连接。

3）域名使用的限制

不得使用或限制使用以下名称（以下列出了一些注册此类域名时需要提供的材料）：

（1）注册含有“China”“Chinese”“CN”“National”等需经国家有关部门（指部级以

上单位）正式批准；

（2）公众知晓的其他国家或者地区名称、外国地名、国际组织名称不得使用；

（3）县级以上（含县级）行政区划名称的全称或者缩写需相关县级以上（含县级）人民政府正式批准；

（4）行业名称或者商品的通用名称不得使用；

（5）他人已在中国注册过的企业名称或者商标名称不得使用；

（6）对国家、社会或者公共利益有损害的名称不得使用；

（7）经国家有关部门（指部级以上单位）正式批准和相关县级以上（含县级）人民政府正式批准是指，相关机构要出具书面文件表示同意 XXXX 单位注册 XXX 域名。例如，要申请 beijing.com.cn 域名，则要提供北京市人民政府的批文。

2．中文域名

英文域名不太符合汉语习惯。随着 Internet 用户爆炸式地增长，这一文化冲突也日益受到重视。1998 年 12 月，第一个中文域名“中国青年报”出现，用户只需在浏览器的地址栏中填入“中国青年报”即可访问《中国青年报》主页。

2000 年 1 月，CNNIC 中文域名系统开始试运行。2000 年 5 月，美国 I-DNS 公司也推出中文域名注册服务。2000 年 11 月 7 日，CNNIC 中文域名系统开始正式注册。2000 年 11 月 10 日，美国 NSI 公司的中文域名系统开始正式注册。这为汉语为母语的人群提供了方便。

中文域名的使用规则基本上与英文域名相同，只是它还允许使用 2～15 个汉字之间的字词或词组，并且中文域名不区分简繁体。CNNIC 中文域名有两种基本形式：

（1）“中文.cn”形式的域名；

（2）“中文.中国”等形式的纯中文域名。

在 http://www.cnnic.net.cn/cdns/reg-manage.shtml 上可以查阅到“中文域名注册管理办法（试行）”。

4.1.3　域名解析

DNS 所提供的服务就是域名与 IP 地址之间的映射——域名解析。

1．域名服务器

Internet 上的主机成千上万，并且还在与日俱增。每个主机具有一个 IP 地址，又有一个域名，从而形成了巨大的名字空间。把巨大的名字空间存放在一个数据库中，由一个服务器进行解析，将会使名字解析的效率低到几乎无法进行的程度。因此，Interent 中的名字信息实际被存储在分布式域名数据库中。这些分布在全球 Internet 中的域名数据库，称为域名服务器或名字服务器（name server）。各域名服务器分布式地存储各自管理的域名信息。

为了管理上的方便，全球的域名服务按照域名空间的层次关系进行组织，并把具有某一后缀的所有计算机组成一个 Zone（区域，网上的结点群）。一个域名服务器可以管理一个或多个 Zone；一个 Zone 管理员必须为所管辖的 Zone 提供一个主域名服务器和至少一个辅域名服务器，以便当主域名服务器出现故障时，不会影响所管辖的 Zone 的服务。

在 DNS 系统中，向域名服务器提出查询请求的 DNS 工作站称为域名解析器（resolver）。为了减少 Internet 上的 DNS 通信量，所有的域名服务器都使用了高速缓存。域名服务器每次收到有关域名的映射信息（主机名和 IP 地址），都会将它们存放在高速缓存中。当有域名解析器提出相同的查询请求时，就可以在高速缓存中直接得到结果，而无须通过域名服务器。只有得到高速缓存中没有要查询的请求时，才去向域名服务器发出查询报文。

同时，所有的域名服务器都是相互链接的。这样，才能让用户快速地找到正确的域名服务器。

2．域名解析的基本过程

DNS 服务器的工作流程称为域名解析过程，它实际上就是一个查询过程。DNS 查询可以根据具体情况采用不同的方式。查询的顺序如下：

① 客户机首先从以前查询获得的缓存信息中查询，查询不到，进入下一步；

② DNS 服务器从自身的资源记录信息缓存中查询，查询不到，进入下一步；

③ DNS 服务器代表请求客户机去查询或联系其他 DNS 服务器，这个过程是递归的，以便完全解析该名称，并随后将应答返回至客户机。

3．域名解析的正向搜索和反向搜索

正向搜索是把一个域名解析成一个 IP。反向搜索正好相反，它是把一个 IP 地址解析成一个域名，常见的诸如 Windows 2003 下的 nslookup 命令工具。由于 DNS 服务是按域名而不是按 IP 地址索引的，反向搜索一搜索就会搜索所有的信息，很消耗资源。为了避免这种情况，DNS 服务创建了一个叫 in-addr.arpa 的特殊二级域，它使用的是与其他域名空间结构相同的方法，但它不采用域名，而是采用 IP 地址。

4. 域名的递归解析与反复解析

当一个客户端发出域名解析请求后，并非任何一个域名服务器都能立刻给出解析结果。在这种情况下，DNS 服务器将接受两种类型的解析：递归解析（recursive resolution）和反复解析（interactive resolution）。它们的解析过程如图 4.2 所示。

当客户端发出递归解析请求后，收到解析请求的 DNS 服务器要么回复一个解析成功的应答，要么继续发出递归解析的请求。

当客户端发出反复解析请求后，收到解析请求的 DNS 服务器要么回复一个解析成功的应答，要么立即回复一个解析失败的应答。客户端收到解析失败的应答后，再向下一个 DNS 服务器发出解析请求。

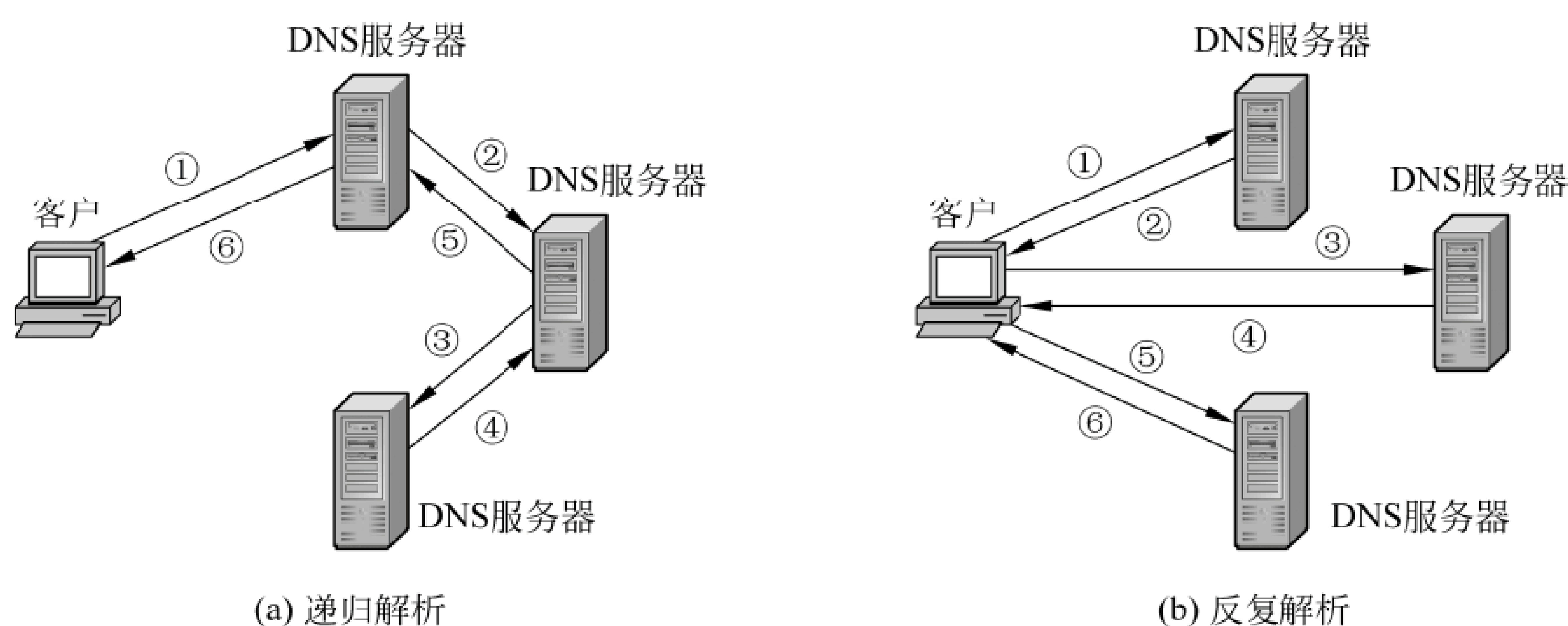


图 4.2　域名的两种解析方法

4.2　文件传输协议

文件传输协议（File Transfer Protocol，FTP）是 TCP/IP 提供的标准机制，用来从一个主机将文件复制到另一个主机。它提供交互式的访问，允许客户指明文件的类型、格式（如是否用 ASCII 等）、存取权限（授权、口令等）。

在网络环境中，由于众多计算机厂商研制的文件系统存在差异，给文件传输带来许多困难：

- 数据存储原型不一致；
- 文件命名规定不一致；
- 对于同一功能，操作命令因操作系统而异；
- 访问控制方法不一致。

FTP 的功能就是减少或消除在不同操作系统下处理文件的不兼容性。

4.2.1　FTP 模型

1．FTP 模型概述

FTP 采用 C/S 模式，如图 4.3 所示为 FTP 的基本模型。

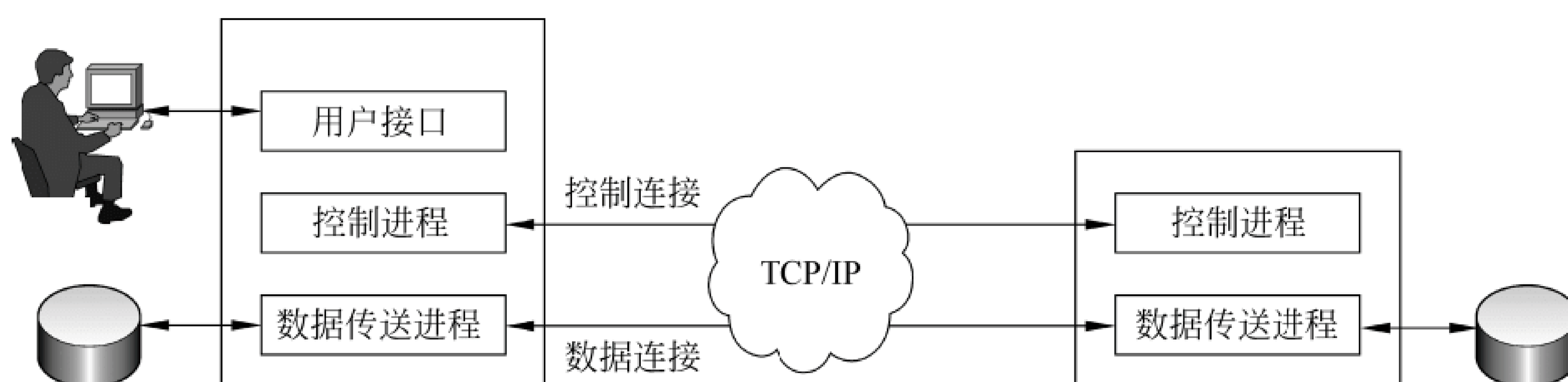


图 4.3　FTP 的基本模型

由图 4.3 中可以看出，一个 FTP 基本模型由如下几部分组成。

（1）两种连接：控制连接和数据连接。

（2）3 个客户组件：用户接口、控制进程和数据传送进程。

（3）两个服务器组件：控制进程和数据传送进程。

2．FTP 连接及其工作过程

FTP 的一个 FTP 服务器进程可以同时为多个客户进程提供服务。FTP 的服务进程由两大部分组成：一个负责接收新请求的主进程；多个处理单个请求的从进程。传送使用 TCP 可靠的传输服务。主进程工作时，要先打开公认端口（21），使客户进程能够连接。然后，主进程与从进程并行地工作：主进程等待并接收客户进程发出连接请求；从进程处理进程发来的请求。从进程对客户进程的请求处理完后即终止，但从进程在运行期间可能会创建其他子进程。

FTP 的一个技术特点是具有两条连接：一条用于数据传送，使用公认端口 20；另一条用于控制信息（命令和响应）的传送，使用公认端口 21。将命令和数据传送分开，将使 FTP 的传送效率更高，并且控制连接与数据连接不会发生混乱。

4.2.2　FTP 文件传输过程

1．数据连接过程

控制进程接收到客户机的文件传输请求后，即创建数据传送进程同时创建数据连接。数据连接创建过程如下：

（1）客户机使用临时端口发出传送文件命令；

（2）客户机将该端口号发给服务器；

（3）服务器发出主动打开命令，建立公认端口 20 与客户机使用的临时端口之间的连接。

此后便由数据传送进程完成文件的传送。传送结束后关闭数据传送连接并结束运行。

2．定义文件属性

在数据传输之前，必须通过控制连接定义要传送文件的 3 个属性。

1）文件类型

- ASCII 文件：这是传送正文文件的默认格式，每一个字符使用 NVT ASCII 进行编码。
- EBCDIC 文件。
- 图像文件：作为连续的比特流传送，没有解释和编码，是二进制文件的默认格式。

若文件为 ASCII 或 EBCDIC 编码，还要定义文件的可打印性。

2）数据结构

- 文件结构（默认）：无结构的字节流文件。
- 记录结构：记录型文件，用于正文文件。
- 页面结构：页面可以顺序地存取。

3）传输方式

- 流方式（默认）：数据以字节流方式由 FTP 交给 TCP，由 TCP 将数据划分为合适大小的报文块。对记录结构，每一记录要增加一个 EOR（记录结束符），文件最后增加一个 EOF（文件结束符）；对文件结构，不需要文件结束符。
- 块方式：数据以块方式由 FTP 交给 TCP。每块前增加 3 字节用作块描述和指示块

大小。

- 压缩方式。

3．确定文件传输方式

- 读取文件：从服务器将一个文件复制到客户机。
- 存储文件：从客户将一个文件复制到服务器。
- 从服务器将目录列表或文件名以文件形式发送到客户机。

4．控制连接上的通信

FTP 控制连接上的通信方法与 Telnet 相同，都使用 NVT ASCII 字符集，并通过命令和响应完成，系统在创建从进程（控制进程）时随之创建控制连接。该控制连接的创建过程如下：

（1）服务器在公认端口 21 发出被动打开命令，等待客户机连接，如图 4.4（a）所示；

（2）客户机使用临时端口发出主动打开命令，如图 4.4（b）所示。

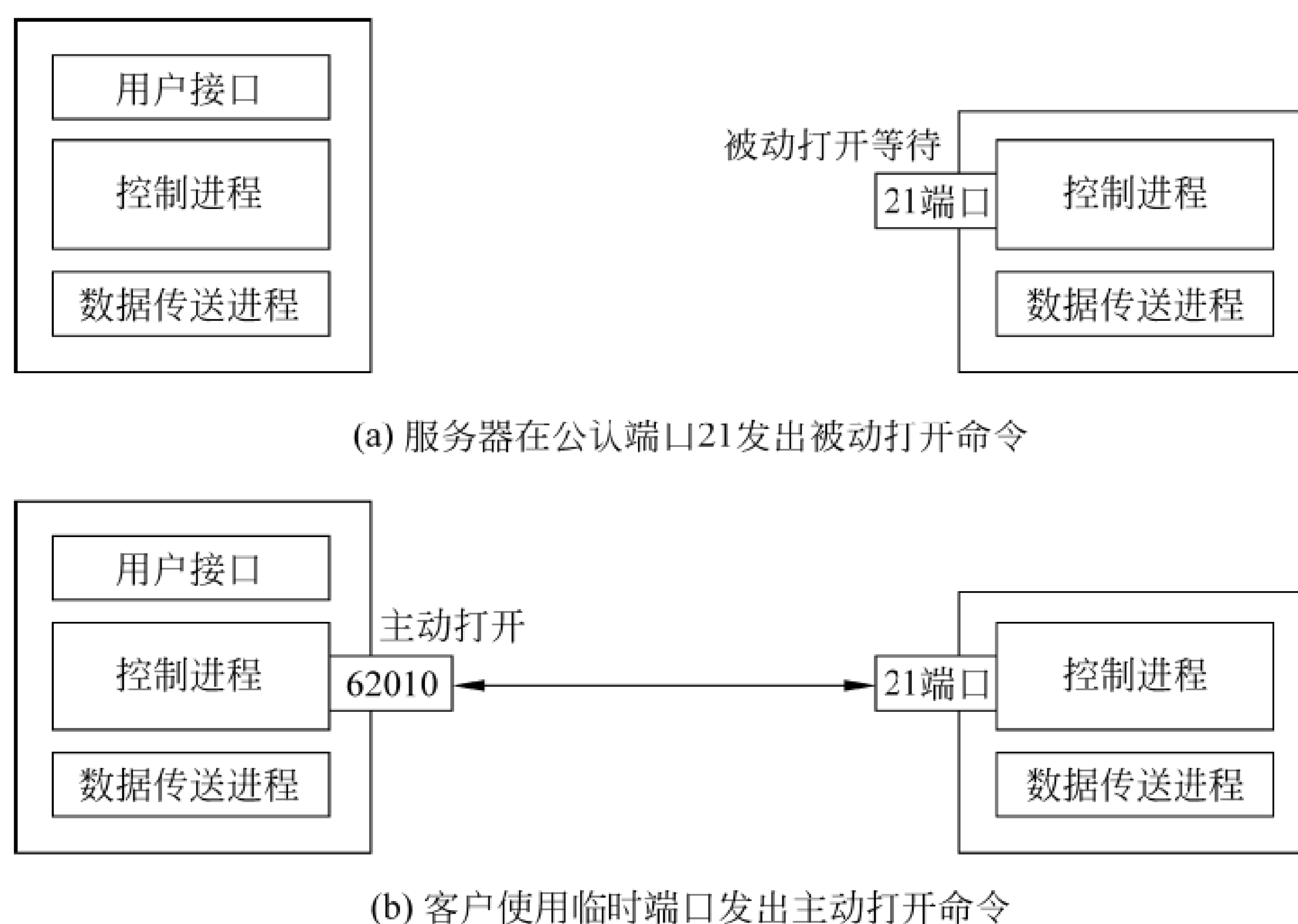


图 4.4　创建控制连接

控制连接在整个会话期间一直打开，随时准备接收客户机的文件传输请求。

在控制连接上传送的是命令与响应。命令由客户发向服务器；响应由服务器发回客户。每一个命令产生至少一个响应。

4.3　超文本传输

4.3.1　超文本与 Web

1．概述

毫无疑问，阅读本书的读者都已经使用过 Internet 上的浏览器了，也体会过浏览时从一

个网页跳跃到另一个网页，从某处跳跃到他处的奇妙功能了，这就是超文本技术。它是指一个含有多个链接（link）的文本文件，每一链接可以指向任何形式的、计算机可以处理的其他信息源，即它可以通过热链接（hotlink）或关键字（词）链接到其他文本、图像、声音、动画等任何形式的文件中，形成一种“联想”关系。一个超文本由多个信息源链接（hyper link）而成，并且这些信息源的数目可以不受限制，从一个文档链接到另一个文档，形成遍布世界的 WWW（World Wide Web，环球信息网）。

WWW 简称 Web，这个名字本身就非常形象地定义了用链接技术组织的全球性信息资源。它所使用的服务器称为 WWW 服务器或 Web 服务器，每个 Web 服务器都是一个信息源。遍布全球的 Web 服务器，通过链接把各种形式的信息，如文本、图像、声音、视频等无缝隙地集成在一起，构筑成密布全球的信息资源。Web 浏览器则提供以页面为单位的信息显示。用户在自己的计算机上安装一个 Web 浏览程序和相应的通信软件后，只需要提出自己的查询要求，就可以轻松地从一个页面跳到另一个页面，从一台 Web 服务器跳到另一台 Web 服务器，自由自在地漫游于 Internet 世界了。用户无须关心这些文件存放在 Internet 上的哪台计算机中，具体到什么地方、如何取回信息都由 Web 自动完成。

2. URL

任何一个信息文档、图像、视频或音频图片都可以被看成是一种资源。为了引用资源，应当使用唯一的标识来描述它放在何处以及软件如何存取它，当前使用的机制称为统一资源定位器（Uniform Resource Locator，URL）。URL 地址既可以是本地硬盘上的某个文件，也可以是 Internet 上的一个网点。

简单地说，URL 由两部分组成：

sckema:path

这里，sckema 表示连接模式。连接模式是资源或协议的类型。WWW 浏览器将多种信息服务集成在同一软件中，用户无须在各个应用程序之间转换，界面统一，使用方便。目前支持的连接模式主要有：HTTP（超文本传输协议）、FTP（远程文件传输协议）、GOPHER（信息鼠）、WAIS（广域信息查询系统）、news（用户新闻讨论组）和 mailto（电子邮件）。

path 部分一般包含有主机全名、端口号、类型和文件名、目录号等。其中主机全名以双斜杠“//”打头，一般为资源所在的服务器名，也可以直接使用该 Web 服务器的 IP 地址，但一般采用域名体系。

path 部分的具体结构形式随连接模式而异，下面介绍两种 URL 格式。

1）HTTP URL 格式

```
http://主机全名[:端口号]/文件路径和文件名
```

由于 HTTP 的端口号默认为 80，因而可以不指明。

2）FTP URL 格式

```
ftp://[用户名[:口令]@]主机全名/路径/文件名
```

其中，默认的用户名为“anonymous”，用它可以做匿名文件传输。如果账户要求口令，口

令应在 URL 中编写或在连接完成后登录时输入。

4.3.2　B/S 计算模式与浏览器结构

1．B/S 模式及其特点

Web 以 B/S 模式（浏览器/服务器模式）工作。B/S 模式是在 C/S 模式基础上发展起来的一种适合 Web 工作的模式。它一方面继承和融合了 C/S 模式中的网络软、硬件平台和应用，又有了一些新的发展和 C/S 模式所不及的特点。下面介绍这些特点。

1）*用户访问方式*

在 C/S 计算模式中，一般采用具有图形用户接口（Graphical User Interface，GUI）的 PC 作为客户机端设备；用户在客户机上以事件驱动方式 1 对 *M* 地访问应用服务器上的资源。

在 B/S 模式中，用户在基于浏览器的客户机上以网络用户界面（Network User Interface，NUI）方式 *N* 对 *M* 地访问服务器上的资源。

2）*体系结构*

通常 B/C 模式采用如图 4.5 所示的浏览器—Web 服务器—应用数据库服务器的三层结构。这时，在用户端只需要安装一个通用的浏览器软件，不需要安装应用软件，就做到了与软、硬件平台无关，为用户提供了方便，并且它的前端是以 TCP/IP 为基础，企业内的 Web 服务器可以接受安装有 Web 浏览程序的 Internet 终端的访问。作为最终用户，只要通过 Web 浏览器，各种处理任务都可以调用系统资源来完成，这大大简化了客户端，减轻了系统维护与升级的成本和工作量，降低了用户的总体拥有成本（Total Cost of Ownership，TCO）。

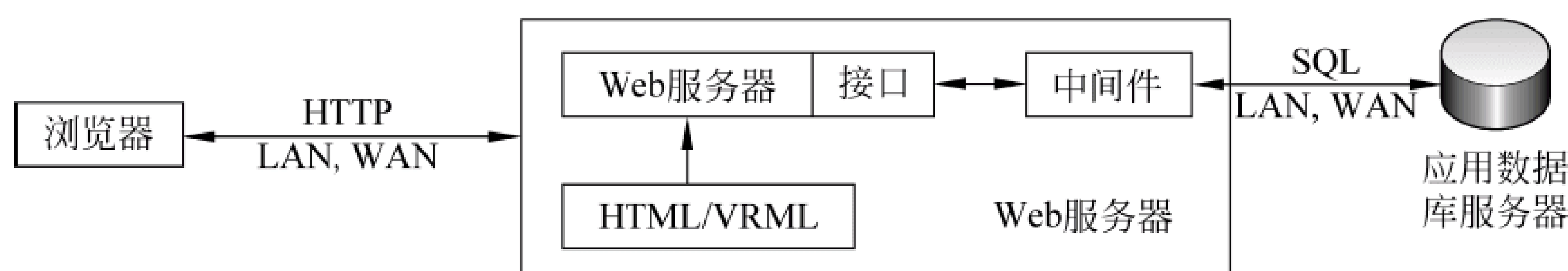


图 4.5　Web 信息服务框架

3）*开发、维护和升级*

在 C/S 模式中，客户端承担着显示逻辑和事务处理逻辑双重功能。系统设计中软件开发的工作量主要在客户端。相对而言，服务器端只承担数据处理逻辑，是一种通用功能，开发相对简单。因此，系统维护的工作量也主要在客户端。

在 B/S 模式中，客户端是一种通用的浏览器，没有多少开发量，主要工作在服务器端。随着软件系统的改进和升级越来越频繁，B/S 架构的产品明显体现出更方便的特性。无论用户的规模有多大，有多少分支机构，都不会增加任何维护升级的工作量，所有的操作只需要针对服务器进行。如果是异地，只需要把服务器连接上网即可进行维护和升级，这对人力、时间、费用的节省是相当可观的。

如表 4.4 所示为 B/S 模式与 C/S 模式特点的对比。

表 4.4 B/S 模式与 C/S 模式特点的对比

	结构	应用软件分布	客户机	客户访问形式	数据流	平台无关性	开发点
C/S	两层结构：客户机-服务器	客户端和服务器端	胖客户机	1:M/GUI	突发性	否	客户机
B/S	三层结构：浏览器- Web 服务器-应用数据库服务器	服务器端	瘦客户机	N:M/NUI	不可预测	是	服务器

2. 浏览器结构

在 B/S 模式中，用户的本地计算机或经远程登录的主机中运行有 Web 的客户程序，即 Web 浏览器。Web 浏览器主要提供两种功能：一方面向用户提供风格统一的、使用方便的信息查询界面；另一方面将用户的信息查询请求转换成 Internet 的查询命令，传送到网上相应的 Web 站点进行处理。Web 服务器完成规定的工作后将所查询结果返回客户机，通过客户程序把返回数据格式化为屏幕显示的格式，显示给用户。客户与 Web 服务器间的交互是通过 HTTP 实现的。

如图 4.6 所示为浏览器的组成。可以看出，一个浏览器有一组客户、一组解释程序、一个管理客户和解释程序的控制程序。

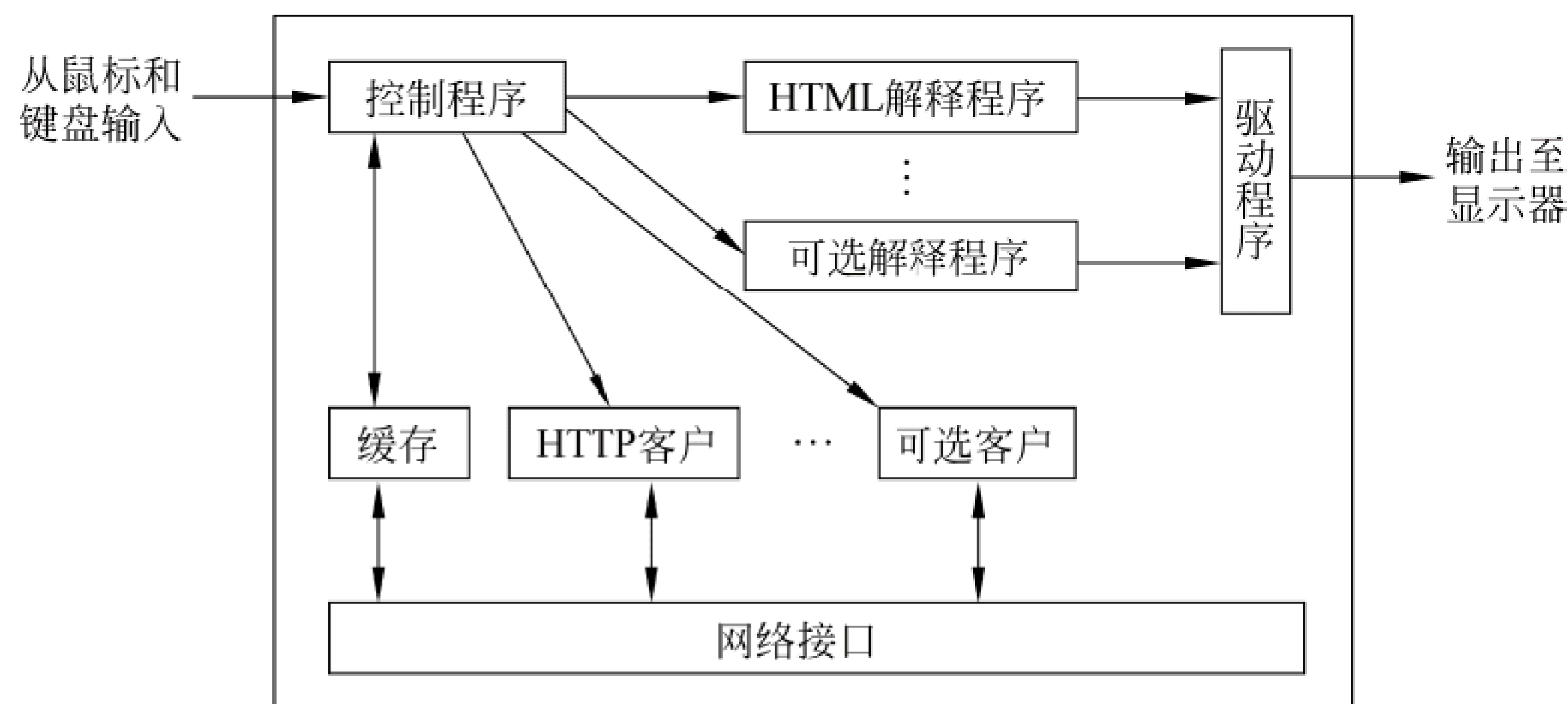


图 4.6 浏览器的主要组成

控制程序是浏览器的核心部件，它解释鼠标命令和键盘输入，并调用有关组件执行用户指定的操作。例如，当用户单击一个链接的起点时，控制程序就调用一个客户程序从远程服务器上将所需文档取回，并调用解释程序向用户显示该文档。

缓存在浏览器中用于存放页面的副本。每当用户单击某一选项时，浏览器首先检查磁盘中的缓存内是否有该项，避免网络过多地传输，以改善浏览器的运行特性。

4.3.3 HTTP 的工作机制

1. HTTP 的特点

在 Web 系统中，浏览器是一个网络客户机，用户可以用它通过 HTTP 并根据某资源的 URL 向 Web 服务器提出请求。Web 服务器一方面通过接口和中间件与网上数据库资源连接，另一方面按用户请求的 URL 将用 HTML/VRML 书写的 HTML/VRML 页面返回给客户端，由浏览器负责解释执行，将最终结果显示在用户面前。因此，浏览器实际上就是一个

HTML/VRML 解释器。

实现 Web 的通信协议 HTTP，是为分布式超媒体信息系统设计的一个协议，它定义了 HTTP 的通信交换机制、请求及响应消息的格式等。

1）以 B/S 模式为基础

HTTP 支持浏览器与服务器之间的通信及相互传送数据。一个服务器可以为分布在世界各地的许多浏览器服务。因而它是一种分布式信息系统，并能对多重协议提供一个统一的通用接口。

2）简易性

HTTP 被设计成一个非常简单的协议，使得 Web 服务器能高效地处理大量请求，客户机要连接到服务器，只需发送请求方式和 URL 路径等少量信息。由于 HTTP 简单，HTTP 的通信与 FTP、Telnet 等协议的通信相比，速度快而且开销小。

3）可扩充性与内容-类型（content-type）标识

HTTP 具有较好的可扩充性，能够支持所有的数据格式，使用该协议传输的信息不仅仅是超文本，也可以是简单文本、声音信号、图像以及可以在 Internet 上访问的任何其他信息，并让客户程序能够恰当地处理它们。

4）短暂连接

短暂连接的含义是限制每次连接只处理一个请求，服务器处理完客户机的请求并收到客户机的应答后，即断开连接，不会继续为这个请求负责，从而不用为保留历史请求而耗费宝贵的资源。这样，实现起来效率十分高，可以节省传输时间。

5）可靠性

HTTP 是一种建立在 TCP 上的协议，它使用 TCP 来确保自身的可靠性。

6）无状态性

HTTP 是一种无状态的协议。无状态是指协议处理事务没有记忆能力。这意味着，由于缺少状态，使得 HTTP 累赘少，系统运行效率高，服务器应答快；另一方面，由于没有状态，协议对事务处理没有记忆能力，若后续事务处理需要有关前面处理的信息，那么这些信息必须在协议外面保存；另外，缺少状态意味着所需的前面信息必须重现，导致每次连接需要传送较多的信息。

2. HTTP 的通信端口

HTTP 通信建立在 TCP/IP 连接上，默认的 TCP 端口号是 80，但也可以使用其他端口号。Web 服务器运行着一个守护进程（HTTP daemon），它始终在端口 80 监听来自远程客户的请求。当一个请求发来时，它就会产生一个子进程来处理当前请求，守护进程继续以后台方式运行，在端口 80 监听来自远程的连接请求。

HTTP 通信中客户提出请求应该带上全部必要的信息，客户机和服务器之间不能对不明确的问题进行磋商。若服务器感到客户提出请求信息不够，无法要求客户给出进一步的信息。

4.4 简单网络管理协议 SNMP

4.4.1 网络管理概述

1. 网络管理的功能

网络管理是为保证网络在使用期内能正常地使用网络服务而进行的全部操作和维护性活动。在 OSI 网络管理框架模型中，基本的网络管理功能被分为如下 5 个方面。

1）配置管理

一个计算机网络是由多种多样的设备连接而成的，它们的参数、状态、名字以及物理结构和逻辑结构，就构成了计算机网络的配置。但是，由于网络运行环境的变化、系统本身用户的增减、以及因设备的维修等原因，为了使网络有效地工作，网络的配置也要随之变化。为此而采取的各种手段就构成了网络管理的配置管理（configuration management）功能。配置管理的主要功能有：

- 识别被管网络的拓扑结构；
- 识别网络中的各个对象；
- 激活跟踪程序；
- 保存网络配置文档、请求服务与服务协议及软件分布情况；
- 动态维护网络的配置数据库；
- 自动修改制定设备的配置。

配置管理的主要目标是有效地维护网络历史的、当前的以及未来的应备配置的详细记录，随时掌握网络的变化或故障可能产生的影响，依据历史记录找出判断和排除网络故障的对策。所以，配置管理是网络管理的基本功能。

2）失效管理

失效管理（fault management）也称故障管理或网络监控，其功能包括主动监控、被动监控（故障检测和诊断）、故障隔离与处理。失效管理的目的是保证网络能提供连续可靠的服务，能快速定位并隔离网络中的故障源或发现潜在的故障，并尽快将其排除。

3）性能管理

失效管理侧重于故障的诊断与排除，而性能管理（performance management）侧重于故障的预防。为了防患于未然，故障管理要收集流量、使用者、访问的资源等信息，并解释周期性性能指标度量和验证网络瓶颈，为未来网络的性能提供预测。其目的是在使用最少的网络资源和具有最小延迟的前提下，保证网络提供可靠和连续的通信能力，并使网络资源达到最优化的程度。

4）计费管理

从本质上讲，计费管理（accounting management）是以网络用户使用网络资源的情况为依据的管理。对于商业化的计算机网络，计费管理要求记录每个用户每次通信的开始时间、结束时间、通信中使用的服务等级、访问的信息资源的类型和流量，以便摊派网络运行费

用，收取回报。从非商业化的目的出发，计费管理的职能是审计，用来统计不同线路的使用情况、不同资源的利用情况等，以便改善网络的运行质量。

5）安全管理

安全管理（security management）具有以下三层含义：

- 保证用户的权益不受损害，如账号被盗用等；
- 保证网络上的信息资源不受侵害，如被窃用、篡改、破坏等；
- 保证网络上的设备不被滥用和破坏。

为了保证网络的安全，除了要采取技术措施、法律手段、道德约束外，还应实施有效的管理措施，这些措施包括：

（1）主动监控措施——利用网络的监测和审计设施，实时记录网络资源的使用情况，报告越轨行为或发出危险行为警报。

（2）被动限制措施——通过对用户注册及其时间、地址位置的限制，对口令进行加密控制，对不良行为加以限制。

（3）防御式补救措施——包括设置资源访问权限、目录与文件属性控制、数据备份与加密等。

一般说来，一个具体的网络管理系统不一定都要包含以上的 5 项功能，不同的系统可能会侧重其中的某几项，但几乎所有的系统都会包括失效管理功能。

2. 网络管理机构

1）IANA

IANA（Internet Assigned Numbers Authority，Internet 编号分配机构）是管理 IP 地址，分配 Internet RFC（Request For Comments）序号以及决定其他与 Internet 运行和服务有关的序号与定义的机构。

2）InterNIC

InterNIC（Internet Network Information Center，网络信息中心）是 IANA 的运行机构，具体负责 IP 地址的分配、域名注册、协调、目录服务、信息统计和发布服务。

但是，由于 Internet 是一个世界范围的计算机互联网络，它按照自治域方式管理和运行不同地域和组织的网络。因此，网络信息中心也是按照自治域和 ISP 分布构建的。

3）NOC

NOC（Network Operation Center，网络运行中心）是各自治域和 ISP 用于完成网络之间的路由、报文转发、计费、安全、与用户相连接以及网络实际运行和维护有关功能的机构。

3. NOC 的管理方式

NOC 对网络和设备的管理方式有以下 3 种。

（1）本地终端方式：通过被管理设备的串行接口，对被管理计算机系统进行监控、配置、计费以及性能和安全管理。

（2）远程 telnet 方式：通过远程登录方式，用命令操作对已知地址和管理口令的设备进行管理。

（3）基于 SNMP 的代理/管理器方式：详细内容将在后面介绍。

4.4.2 SNMP 管理模型

SNMP（Simple Network Management Protocol，简单网络管理协议）是使用 TCP/IP 协议族对 Internet 上的设备进行管理的一个框架，它提供一组基本的操作对 Internet 进行监视和维护，并使用两个基本的概念——管理器（manager）和代理（agent）。如图 4.7 所示，一个网络管理系统由管理站、代理设备和被管理设备三者组成。被管设备可以是网络中的任何类型的结点，包括计算机、通信服务器、打印机、路由器、网桥和集线器等。代理设备是运行 SNMP 服务器程序的主机或路由器，它随时记录网络上的各种事件，并随时向管理器报告网络的使用情况以及各项参数。管理器是运行 SNMP 客户程序的主机，获得代理提供的有关信息后，向代理程序下达有关命令，对网络进行适当调整，使网络达到最佳运行状态。由于有些被管设备运行网管软件的能力有限，因此必须设定一个最低基准，定义一个最基本的性能指标。

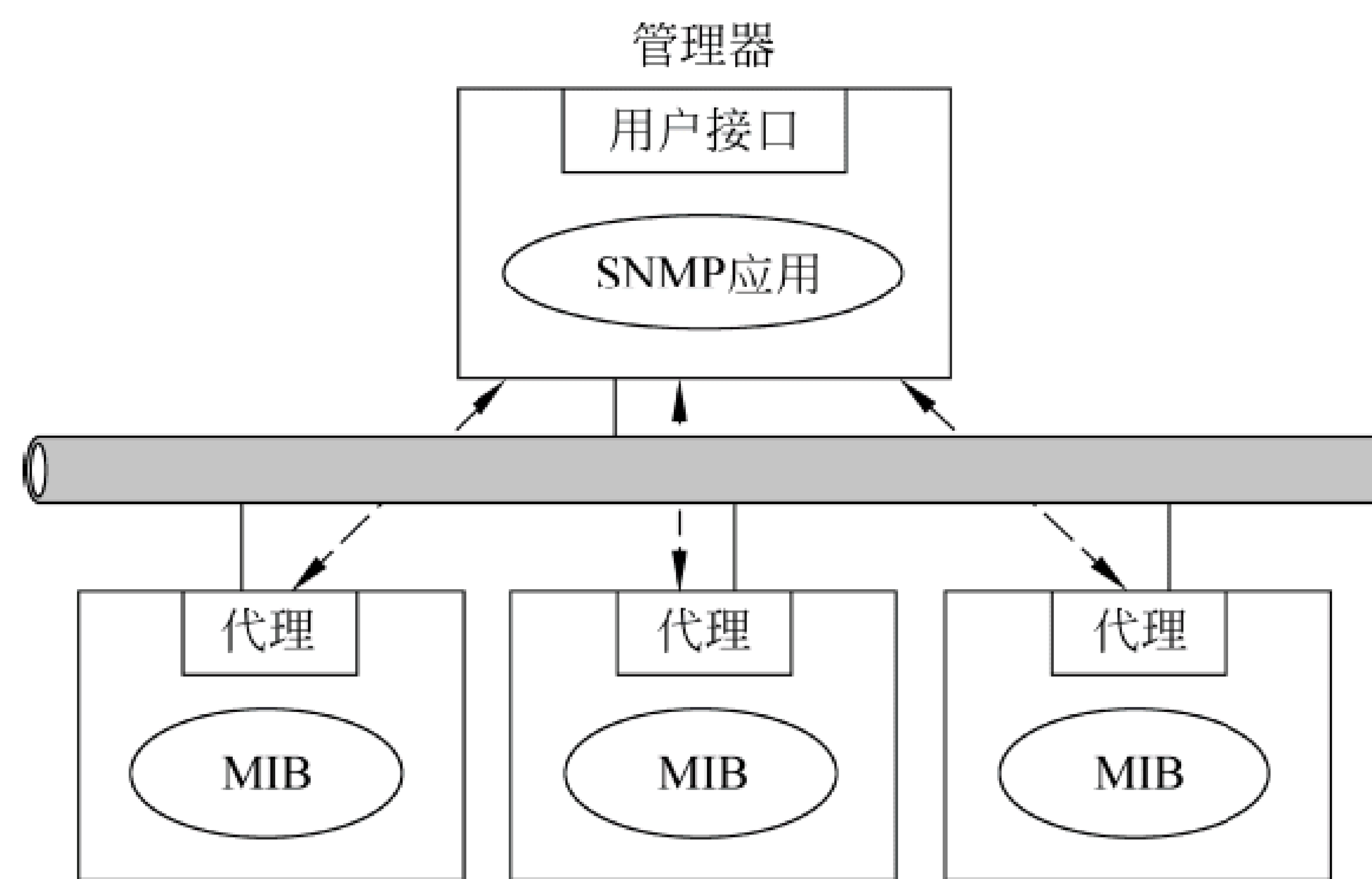


图 4.7　SNMP 管理模型

注意：管理器是通过发出请求得到能够反映代理行为的信息进行检查，所以它是一个客户端，而代理是服务器端。

此外，Internet 中的管理不仅是通过 SNMP 完成的，还要使用另外一些协议，其中主要是管理信息标准（Standard of Management Information，SMI）和管理信息库（Management Information Base，MIB）。

4.4.3 SMI

SMI 是 SNMP 的一个指南，它给出描述管理对象 3 个属性的标准：

- 给对象命名的方法；
- 定义可以在对象中存储的数据类型的方法；
- 对在网络上传输的数据进行编码的方法。

SMI 的详细定义在 RFC1155 中。下面仅简要介绍。

1. 名字

SMI 要求每一个被管对象（如一个路由器、一个路由器中的变量、一个值等）具有一

个唯一的名字。为了使名字具有全局性，如图 4.8 所示，SMI 采用了基于树结构的分级命名体制，并且可以采用点分十进制或点分名字的记法。

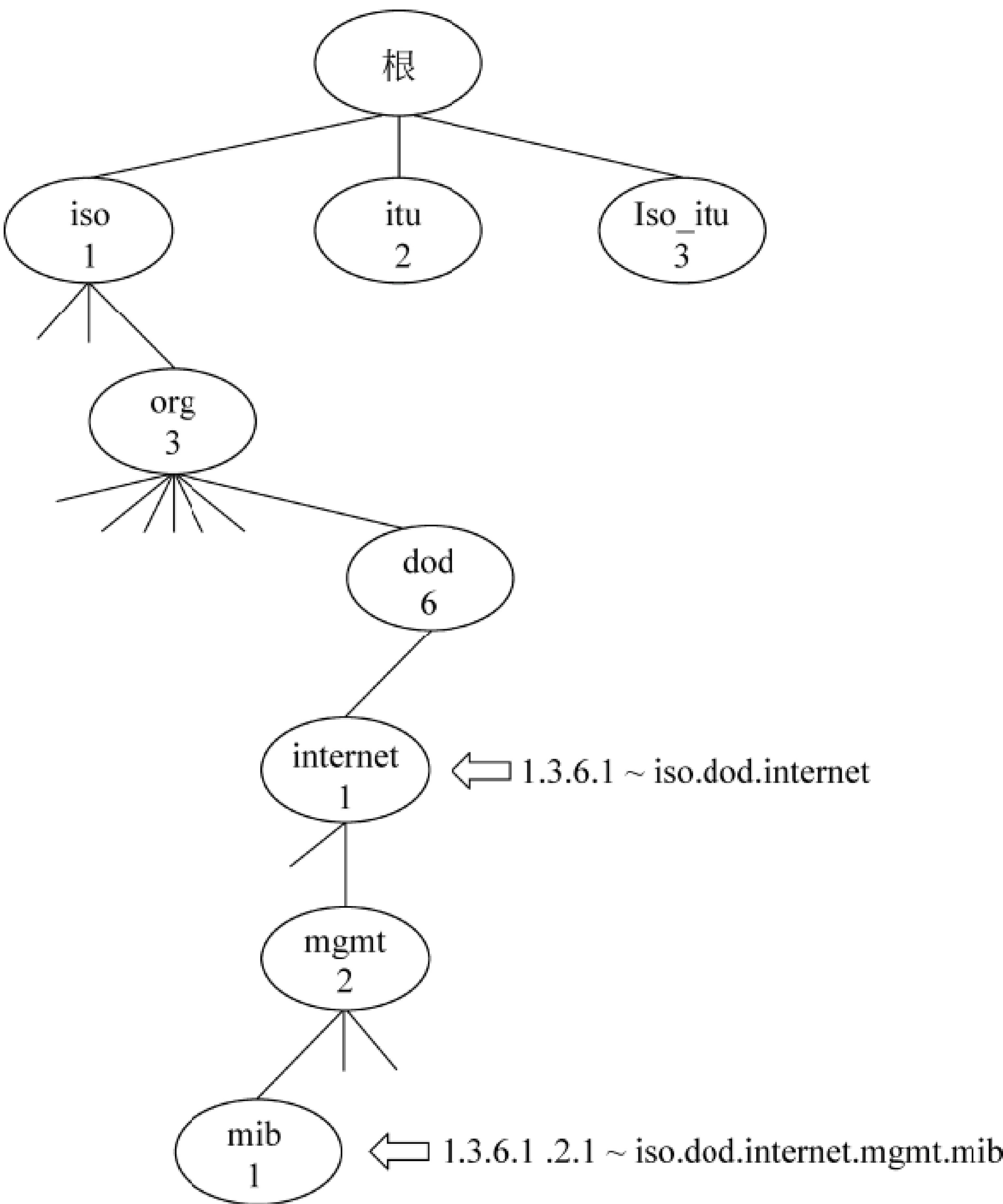


图 4.8　SMI 基于树结构的分级命名体制

2. 类型

SMI 定义对象存储的数据的数据类型的方法是基于 ASN.1 的，并且分为两大数据类型：简单类型和构造类型。

1）简单类型

简单类型是原子类型，表 4.5 中列出了 7 种重要简单数据类型。

2）构造类型

SMI 定义了两种构造数据类型。

- Sequence：一些简单数据类型（不要求相同）的组合。
- Sequence of：一些相同数据类型的组合。

表 4.5　SMI 定义的重要简单数据类型

类　型	大　小	说　明
Interger	4 字节	在 0 到 2^{32}–1 之间的一个基数
String	可变	零个或多个 ASCII 字符
ObjectIdentifier	可变	用 ASCII 数字表示的对象标识符
IPAddress	4 字节	由 4 个整数组成 IP 地址
Counter	4 字节	一个整数，其值可从 0 增加到 4 294 967 295；当它到达最大值时就返回到 0
Gauge	4 字节	与 Counter 相同，但当它到达最大值时，它不返回；它保持在这个数值直到复位
TimeTicks	4 字节	记录时间的计数值，以 1/100s 为单位

3. 编码

SMI 使用基本编码规则 BER，将数据编码后在网络上传输。BER 要求每一块数据都要编码成如图 4.9 所示的三元组格式：标记、长度和值。

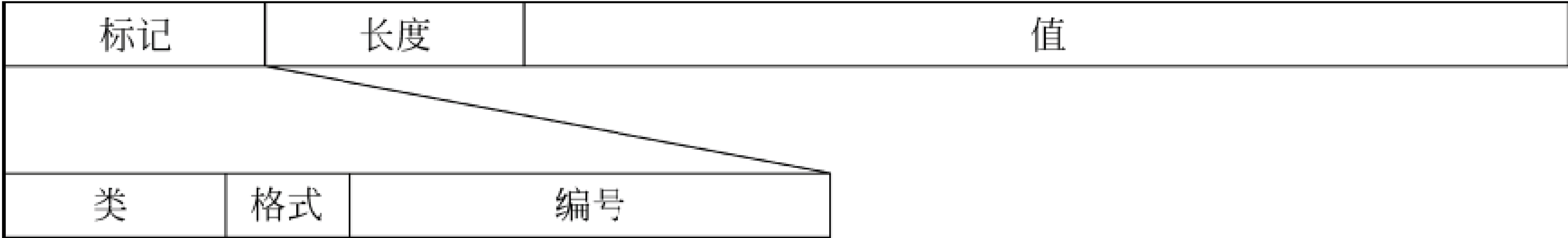


图 4.9　SMI 数据编码格式

（1）标记。标记是一个描述数据类型的 1 字节字段。它由 3 个子字段组成：

- 类（2bit）定义数据的作用域，分为：通用类（00）、应用类（01）、特定上下文类（10）和专用类（11）。
- 格式（1bit）指出数据是简单数据类型还是构造数据类型。
- 编号（5bit）将数据类型进一步编号。

（2）长度。长度为一个字节或多个字节。若为一个字节，其最高位必为 0；若为多个字节，则前面的几个字节的最高位必为 1，以说明后面的字节还是长度子字段，最后字节的最高位为 0。

（3）值。值字段按照 BER 中定义的规则编码。图 4.10 为几个 SMI 数据编码的例子。

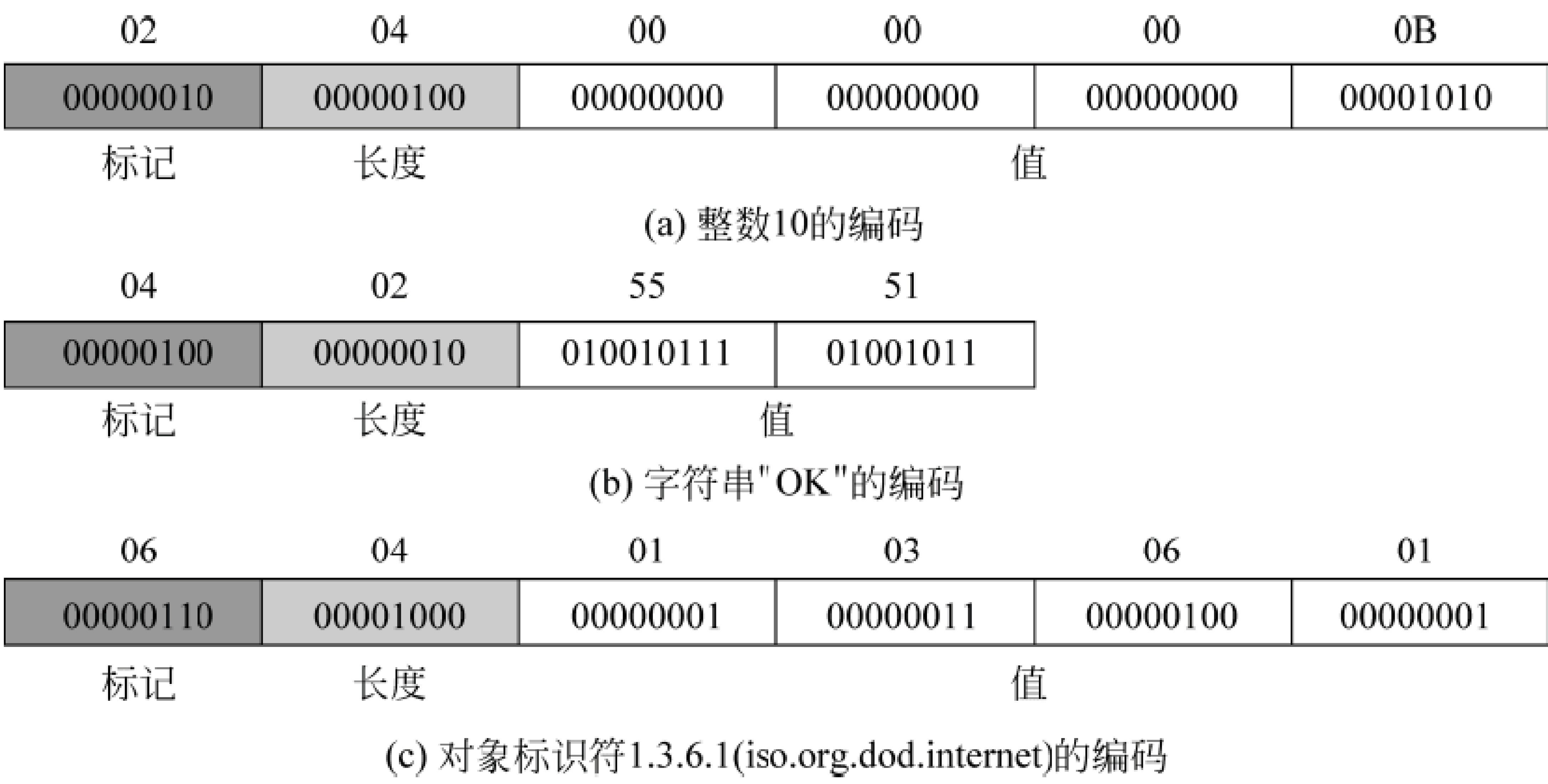


图 4.10　SMI 数据编码示例

4.4.4　MIB

1. MIB 概述

MIB 是管理器能管理对象的集合。每一个代理都有自己的 MIB。MIB 中所有对象的定义规则和语法，都在 SMI 中有详细的描述，并且应当具备如下几个项目：

- 对象名称；
- 对象类型；
- 访问状态：对象是只读、只写或可擦写等；

- 对象描述：描述对象的各种信息，如设备规格等可提供管理器解读的数据；
- 对象识别码：即 OID 对象识别码，用于保证对象在 MIB 中的唯一性。

MIB 有许多版本。其中，ISO 制定的 MIB-Ⅰ和 MIB-Ⅱ是两个重要的标准。

2. MIB-Ⅱ

MIB-Ⅱ是 SNMP 协议进行管理时所运用的变量集合的定义标准，也是使用性最高的网络数据结构标准。图 4.11 为 MIB-Ⅱ对象标识码树结构。例如，Internet 对象的 OID 定义便为{ISO(1) ORG(3) DOD(6) Internet(1)}，即 1.3.6.1。

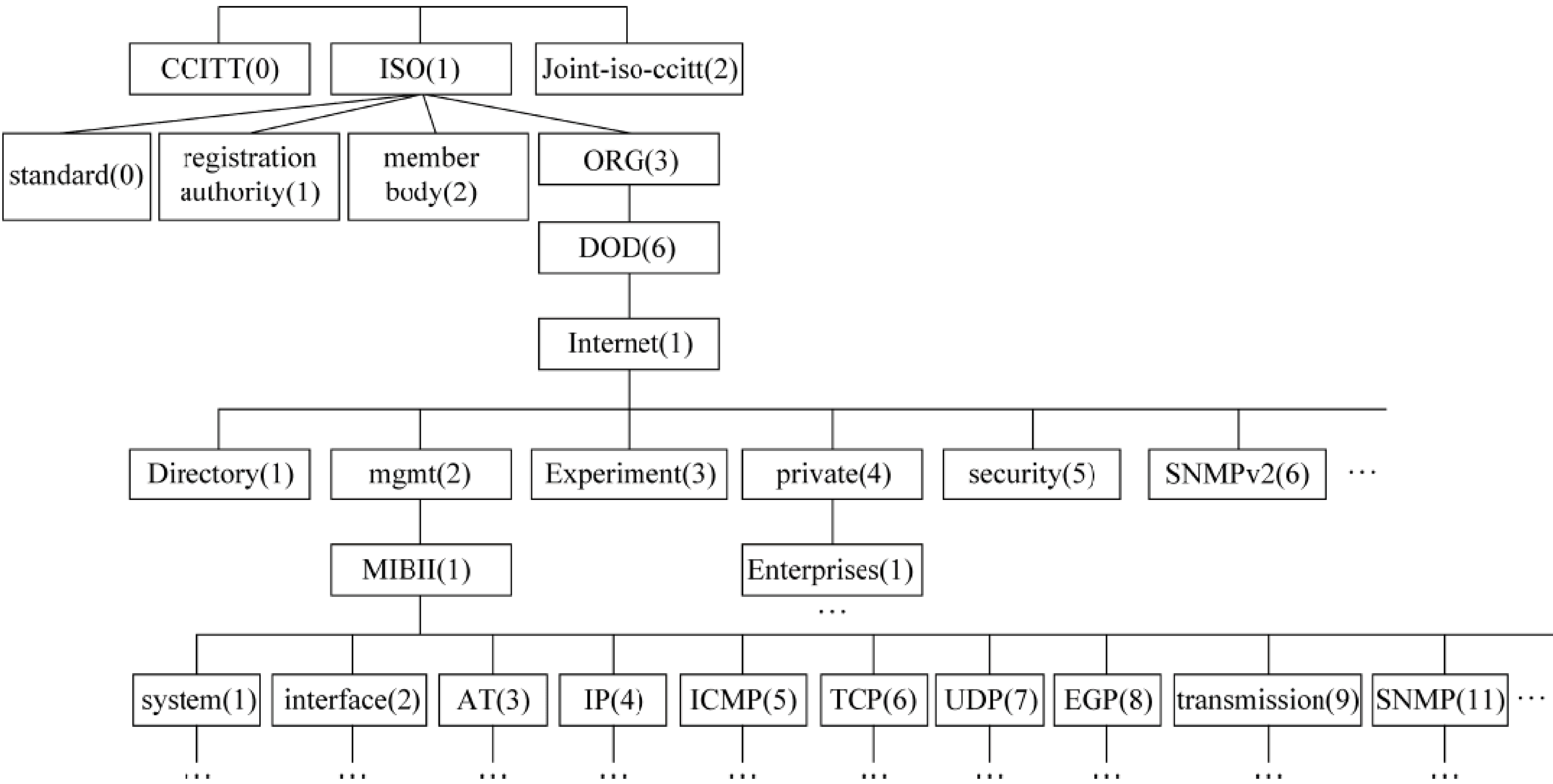


图 4.11　MIB-II 对象标识码树结构

MIB 将所有管理的对象都按一定的标准分为不同的群组。图 4.11 中的最下面一行便是 MIB-Ⅱ定义的各功能群组。表 4.6 为对一些重要的 MIB-Ⅱ功能群组的说明。

表 4.6　较重要的 MIB-Ⅱ功能群组

群组名称	对象数量	说　明
system	7	描述设备名称（sysName）、识别码（sysObjectID）、激活所需时间（sysUpTime）、管理者名称（sysContact）、位置（sysLocaton）、定义（sysDesct）、网络层级（sysServices）
internet	23	描述网络装置接口的各项数据及网络接口个数，前缀为 if。如 ifNumber（网络接口个数）
AT	3	地址转译，如地址解析的相关信息，前缀为 at
IP	42	描述与 IP 相关的流量、寻址、重组、舍弃等信息，前缀为 ip
ICMP	26	包含 ICMP 的各项信息：网络状态、错误、计数等，前缀为 icmp
TCP	19	描述 TCP 协议连接、送收、错误等信息。前缀为 tcp
UDP	7	描述 UDP 协议送收包数量、故障原因等信息，前缀为 udp
EGP	20	描述外部网关和；路由器的各项信息，前缀为 egp
transmission	0	保留给特定媒体
SNMP	30	描述 SNMP 协议运作、信息数量各项信息统计，前缀为 snmp

4.4.5 SNMP 的工作机制

1. UDP 端口

SNMP 在两个公认端口 161 和 162 上使用 UDP 服务。公认端口 161 由服务器（代理）使用，162 由客户（管理器）使用。

2. 管理器轮询，代理报告异常

SNMP 协议是一个异步的请求/响应协议，它的管理功能是通过轮询操作实现的。管理器周期地向被管设备的代理发送轮询信息，并根据各代理回复的响应进行处理。这时，代理（服务器）在端口 161 上发出主动打开，然后等待；而管理器（客户）使用短暂端口发出主动打开。客户向服务器发送请求报文，以短暂端口为源端口，以公认端口为目的端口；服务器向客户发送响应报文，以公认端口为源端口，以短暂端口为目的端口。

除了管理器发送轮询信息外，被管设备也通过代理发送异常信息来中断管理器的工作处理流程。

这种管理器周期地发送轮询信息以监视和维持网络资源，被管设备的代理进行异常报告的机制，使 SNMP 成为一种实现简单、维护容易和非常有效的管理协议。

3. SNMP 的通信原语

SNMP 使用 5 种原语实现网络管理功能。

（1）get_request：访问代理，并从 MIB 表上得到指定的对象实例值；

（2）get_response：响应管理器来的请求，包含响应标识和响应状态信息；

（3）get_next_request：访问代理，并从 MIB 树上检索指定对象的下一个对象实例；

（4）set_request：描述在一个对象实例上的执行行动；

（5）trap：代理向管理器发送异常事件。

4. 格式

SNMP 报文的前 4 种格式相似，如图 4.12（a）所示；唯 trap 报文格式有所不同，如图 4.12（b）所示。

下面对 SNMP 格式中的有关字段做扼要介绍。

（1）版本（Version）：实际值为版本号减 1。

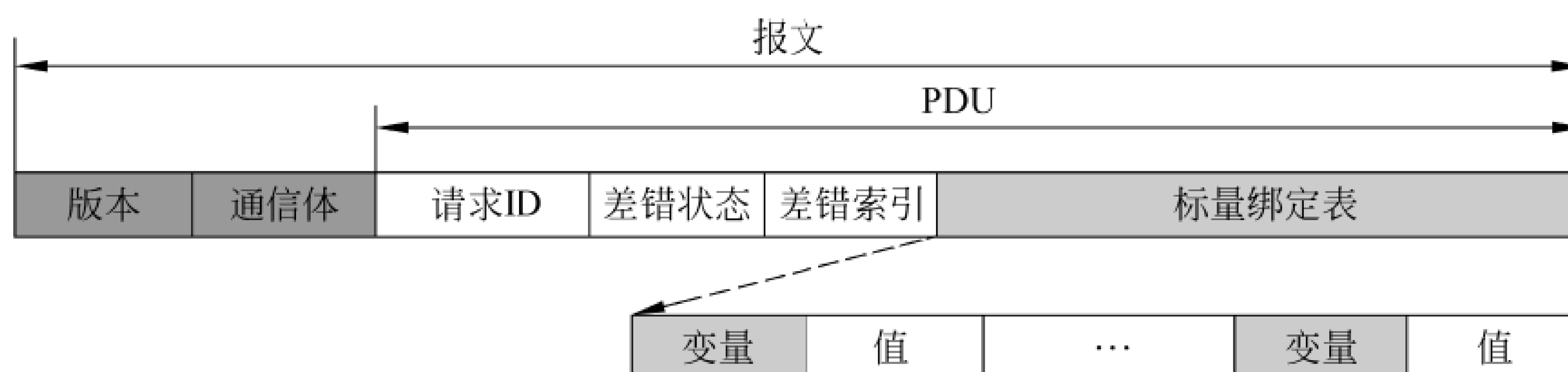
（2）通信（Community）：定义口令。默认为 public。

（3）请求标识（Request ID）：管理器在请求报文中使用的一个序号，代理将在响应中重复。

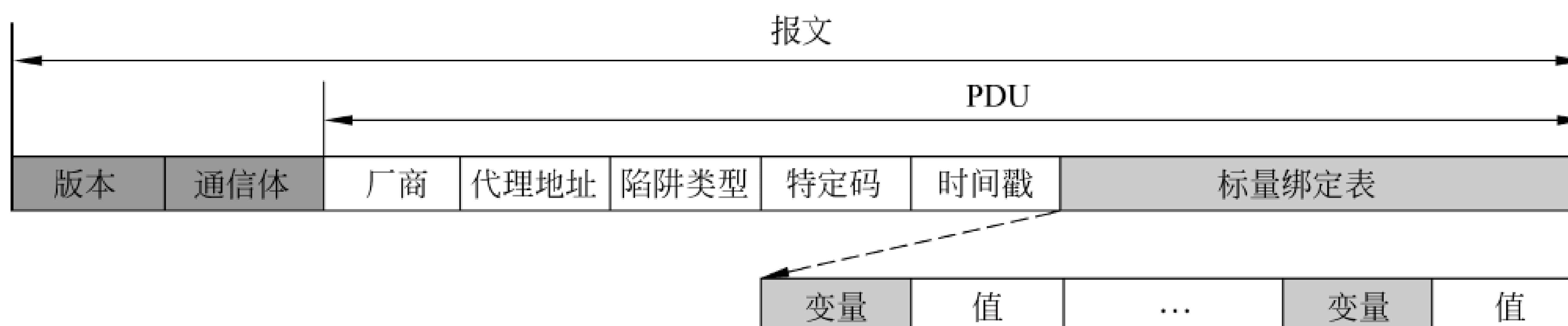
（4）差错状态（Error status）：只用于响应报文，给出代理报告的差错的类型。在请求报文中为 0。可能出现的差错类型有如表 4.7 所示的几种。

（5）差错索引（Error index）：是一个偏移，告诉管理器引起差错的是哪个变量。

（6）变量绑定表（VarBindList）：管理器希望读取或设置的一组具有对应值的变量。



(a) get_request\get_request、set+request和get_response报文格式



(b) trap报文格式

图 4.12　SNMP 报文格式

表 4.7　可能出现的差错类型

状　态	名　称	意　义
0	noError	无差错
1	tooBig	响应太大，无法放进一个报文内
2	noSuchName	变量不存在
3	badName	要存储的值无效
4	readOnly	企图修改只读对象
5	genErr	其他

（7）厂商（Enterprise）：定义产生陷阱的软件包的标识（ObjectID）。

（8）代理地址（Agent address）：定义陷阱的代理的 IP 地址。

（9）陷阱类型（Trap type）：这些类型如表 4.8 所示。

（10）特定码（Specific code）：陷阱类型为 6 时，定义厂商使用的特定码。

（11）时间戳（Time stamp）：给出引起陷阱的事件所经历的时间。

表 4.8　陷阱类型

状　态	名　称	意　义
0	coldStart	代理已被引导
1	wanmStart	代理已被重新引导
2	linkDown	接口出故障
3	linkUp	接口已正常工作
4	authenticationFailure	检测出无效通信体
5	egpNeighborLose	EGP 路由器变为故障状态
6	enterPriseSpecifie	其他报文

5. 编码

1）报文结构

如图 4.12 所示，一个报文是一个三元组：版本、通信体和 PDU。它们又各是一个三元组：

- 版本：标记、长度和值；
- 通信体：标记、长度和值；
- PDU：代码、长度代码和 PDU 数据代码。

而 PDU 数据又包括请求 ID（标记、长度和值）、差错状态、差错索引和变量绑定。

2）编码规则

SNMP 采用 BER 标准对报文进行编码，并且采用如下规则：

- 报文用标记定义；
- 类是上下文敏感的（context-sensitive，值为 10）；
- 格式是结构化的（取 1）；
- 编号因报文类型分别为：0（00000）、1（00001）、2（00010）、3（00011）、4（00100）。

下面是不同类型的报文的整个标记。

- get_request: A0(10100000)；
- get_next_request：A1(10100001)；
- get_response: A2(10100010)；
- set_request: A3(10100011)；
- trap: A4(10100100)。

6. 举例

管理器（SNMP 客户）发送 get_request 报文，希望知道一个特定的路由器已经收到了多少 UDP 数据报；代理用 get_response 报文响应。

1）get_request 报文

要发送报文获知路由器已经收到了多少 UDP 数据报，与此信息相关的响应是 udpInDatagram，其标识符为：1.3.6.1.2.1.7.1。由于管理器打算读取一个值，因此最后一部分定义一个值为 0 的空实体。报文编码如下：

```
30 2A                                   Sequence,长度为 2A16
  02 01 00                              Integer, 长度为 0116, 版本=0
  04 06 70 75 62 6C 69 63               String, 长度为 0616, 通信体为默认: "public"
  A0 1D                                 get_request, 长度为 ID16
    02 04 00 01 06 11                   Integer, 长度为 0416, 请求 ID=0001061116
    02 01 00                            Integer, 长度为 0116, 差错状态=0016
    02 01 00                            Integer, 长度为 0116, 差错索引=0016
    30 0F                               Sequence, 长度为 0F16
      30 0D                             Sequence, 长度为 0D16
        06 09 01 03 06 01 02 07 01 00   ObjectID, 长度为 0916,udpInDatagram
        05 00                           空实体,长度为 0016
```

2）get_response 报文

用来送出所收到的 UDP 数据报数量。与之相关联的 MIB 变量也是 udpInDatagram，而 VabBindList 是对象标识符，其后跟对象的值。报文编码如下：

```
30 2E                                  Sequence,长度为 2E16
  02 01 00                             Integer,长度为 0116， 版本=0
  04 06 70 75 62 6C 69 63              String， 长度为 0616， 通信体为默认:"public"
  A0 1D                                get_request， 长度为 2116
    02 04 00 01 06 11                  Integer,长度为 0416， 请求 ID=0001061116
    02 01 00                           Integer,长度为 0116， 差错状态=0016
    02 01 00                           Integer,长度为 0116， 差错索引=0016
    30 0F                              Sequence， 长度为 1316
      30 0D                            Sequence， 长度为 1116
        06 09 01 03 06 01 02 07 01 00  ObjectID， 长度为 0916， udpInDatagram
        05 00                          Counter， 长度为 0416， 值 12 11
```

4.5　电 子 邮 件

电子邮件（E-mail）是 Internet 上一种最广泛的应用。Internet 的电子邮件系统采用了 C/S 方式，电子邮件的发送与接收由 E-mail 客户程序和服务程序共同完成。

4.5.1　电子邮件系统的基本原理

1．电子邮件系统的一般构成

电子邮件系统的一般结构如图 4.13 所示，其最主要的部件是用户代理（User Agent，UA）和邮件传送代理（Mail Transfer Agent，MTA）。

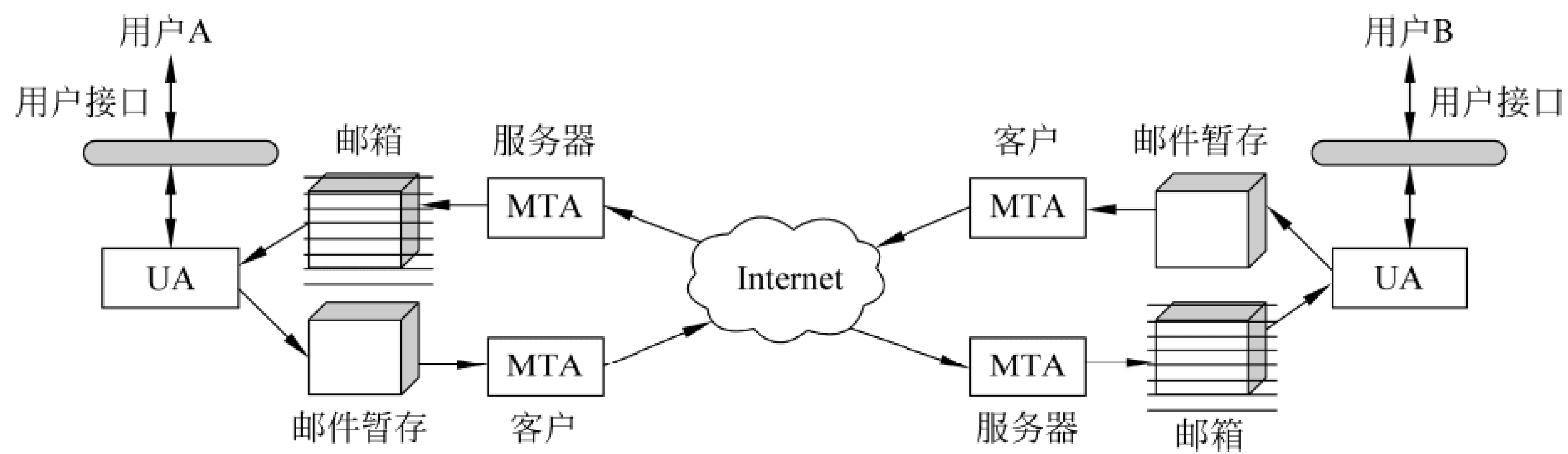


图 4.13　E-mail 的客户机/服务器工作方式

1）用户代理（UA）

UA 通常是一个用来发送和接收邮件的程序。它的主要功能如下。

- 发送邮件：UA 为用户准备报文、创建信封，并将报文装进信封，暂存起来。
- 接收邮件：UA 定期检查邮箱，若有邮件到来，就向用户发出一个通知；若用户打开信箱准备读取邮件，则显示一个清单，给出邮件的有关信息，包括发信人地址、主题、发送时间等。

有些用户代理具有额外的用户接口，向用户提供可视化的交互服务。

2）邮件传送代理（MTA）

MTA 相当于现实生活中的邮局，担任邮件传送工作。MTA 分为客户机 MTA 和服务器 MTA。客户机 MTA 的功能是将暂存的邮件传送到 Internet 上；服务器 MTA 的功能是将 Internet 上送来的邮件传送到客户端的邮箱中。

2. 电子邮件访问模式

电子邮件一旦被传送到邮件存储服务器后，接收者就可以访问它。接收者对电子邮件服务器的访问方式有 3 种：离线（offline）、在线（online）和断线（disconnected）。

1）离线模式

离线模式是最基本的模式。按照该模式工作时，客户机与邮件存储服务器相连接后，下载所有的接收者邮件，同时从服务器中删除；然后在本地客户机上存储、处理。这种模式简单，仅需要最小的服务器连接时间。

2）在线模式

在线模式中所有的邮件处理和操作都在服务器上进行（尽管在某些情况下用户可以把邮件下载到本地客户机，但服务器中仍然保留）。当用户需要访问并处理电子邮件时，必须与服务器保持连接。这样，客户机的配置可以很小，但服务器需要有足够的带宽和资源供多个用户分享。

3）断线模式

断线模式综合了离线模式和在线模式的特点。在这种模式中，用户能下载邮件在本地客户机上离线处理，但服务器仍然是邮件的保存处。用户处理完邮件后，可再次与邮件服务器连接并上传所有的改变。采用这种模式，客户机与服务器的连接时间更短，但不论客户机还是服务器都需要足够的资源。

4.5.2 简单邮件传输协议

简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）是 Internet 上各 MTA 站点之间的电子邮件传送协议。SMTP 主要用于连接建立、邮件传送和连接释放。一个邮件报文的传送过程需要经过 3 个阶段。

① 建立连接。在使用 SMTP 进行邮件传送过程中，客户机（发送）端使用短暂端口，服务器（接收）端使用公认端口 25。当客户与服务器的公认端口 25 之间建立了一条 TCP 连接后，SMTP 服务器就开始其连接阶段。

② 传送报文。SMTP 在客户与服务器之间建立连接后，发信人就可以向一个或多个收信人发送一个单独的报文了。

③ 终止连接。报文传送成功后，客户就可以终止连接。

4.5.3 其他几个重要的电子邮件协议

1. 通用 Internet 邮件扩充标准（MIME）

MIME（multipurpose internet mail extensions）是一个辅助协议，它允许非 ASCII 数据通过 SMTP 传送。为适应任意信息数据类型的表示，每个 MIME 报文要包含告知收信人数据类

型和所使用编码的信息。基本内容类型（Content-Type）用于说明邮件的性质。表 4.9 所示为 7 种基本内容类型及其说明。

表 4.9　7 种基本内容类型及其说明

基本内容类型	子　类　型	说　　明
text	plain	无格式文本
	richtext	有少量格式命令的文本
image	gif	GIF 格式静止图像
	jpeg	JPEG 格式静止图像
audio	basic	可听见声音
video	mpeg	MPEG 格式影片
application	octet-stream	不间断字节序列
	postscript	PostScript 可打印文件
message	rfc822	MIME RFC 822 邮件
	partial	为传输而分割开的邮件
	external-body	从网上获取文件
multipart	mixed	按规定顺序的几个独立部分
	alternative	不同格式的同一文件
	parallel	必须同时读取的几部分
	digest	每一部分都是完整的 RFC 822 邮件

2．邮局协议（POP）和 Internet 报文存取协议（IMAP）

以拨号连接方式进行电子邮件传送的用户一般都要使用 POP（Post Office Protocol）。这种情况下，用户要先拨号，与邮箱所在的计算机建立连接；连接成功就可以运行 POP 客户程序，与远地的 POP 服务器程序通信，发送或接收电子邮件。

POP 是一个离线协议，它是一个具有存储转发功能的中间服务器，用户每次打开邮箱，即将邮箱中接收到的邮件一次性取回到自己的计算机，POP 服务器就不再保存这些邮件，用户与 POP 服务器的连接即中断。此后，用户便可以在自己的计算机上自由地处理收到的邮件。

IMAP（Internet Message Access Protocol）是美国斯坦福大学从 1986 年就开始开发的与 POP3 对应的一种多重邮箱电子邮件协议。它能从邮件服务器上获取有关 E-mail 信息或直接收取邮件，具有高性能和可扩展的优点。它提供在线、离线、断线 3 种操作模式，使用户可以在远地操纵服务器邮箱。所有收到的邮件要先送到 IMAP 服务器，用户需要打开某个邮件，才能将该邮件传到自己的计算机中，在用户未发出删除该邮件的操作之前，它一直保存在 IMAP 服务器上。显然，使用 IMAP 与使用 POP 相比，用户与服务器的连接频繁且时间长。

应当注意，IMAP 和 POP 是用户与本地邮件服务器之间的邮件传送协议，而 SMTP 是 Internet 上各 MTA 站点之间的电子邮件传送协议。

3. 邮件转发

邮件转发（mail forwarding）软件可以将邮件中使用的邮件地址映射为一个或多个新的邮件地址。此外，它还包含一个邮件别名扩展（mail alias expansion）机制。使用别名系统允许单个用户拥有多个邮件标识符，于是就可以建立一些邮件发送清单（mailing list）使一个标识符与一批收信人相关联，利用邮件分发器（mail exploder）将接收到的一个邮件发送给一大批人。在 Internet 上有许多开放的邮件发送清单。

4. 电子邮件网关

SMTP 并非唯一的电子邮件协议。如图 4.14 所示，当一个专用网中不使用 TCP/IP 时，其所使用的电子邮件协议也会与 SMTP 不同。这时可以通过电子邮件网关（E-mail gateway）实现不同协议之间的转换，将一种格式的邮件转换成另一种格式。

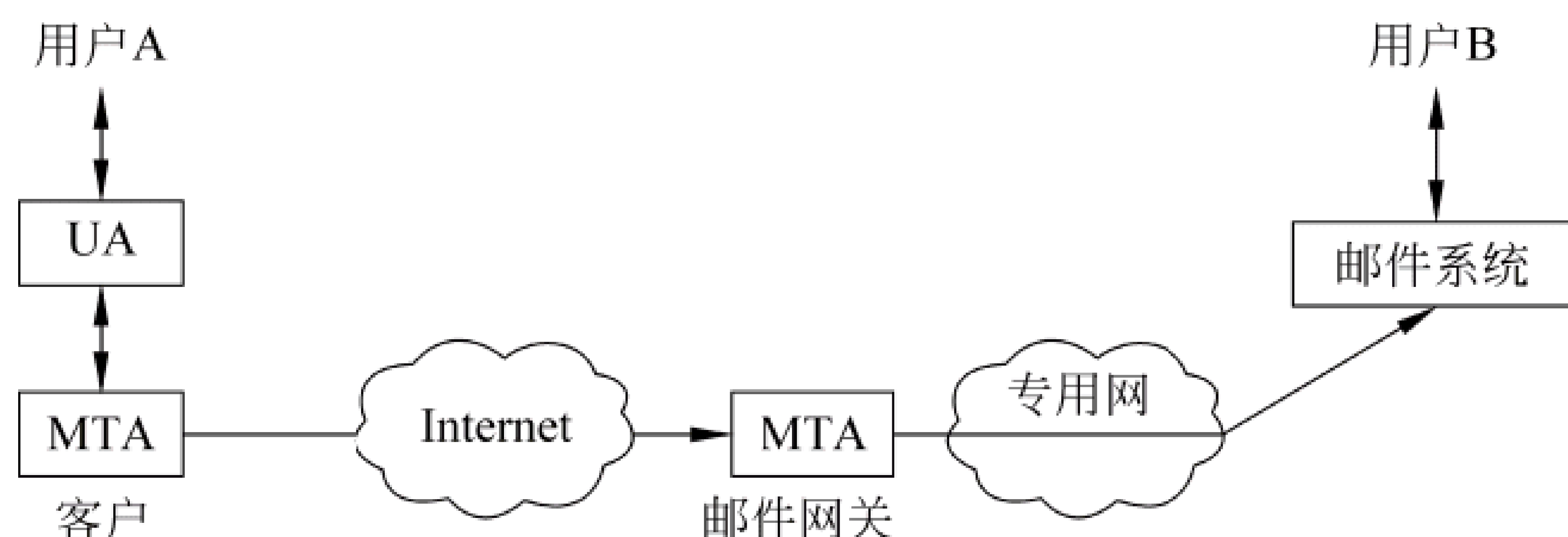


图 4.14　电子邮件网关的工作过程

4.6　网络交流平台

网络交流平台就是以互联网作为交流分享的平台，综合利用网络载体，达到双方思想交流。运用 BBS、E-mail、即时通信软件、BLOG（博客）等网络交流载体，提高交流的广泛性，最大限度地实现社会化网络信息的可选择性和平等性。

4.6.1　即时通信软件

即时通信（Instant Messaging，IM）是指能够即时发送和接收互联网消息等的业务。自 1998 年面世以来，特别是近几年的迅速发展，即时通信的功能日益丰富，逐渐集成了电子邮件、博客、音乐、电视、游戏、搜索等多种功能。即时通信不再是一个单纯的聊天工具，它已经发展成集交流、资讯、娱乐、搜索、电子商务、办公协作、企业客户服务等为一体的综合化信息平台。

即时通信软件除了可以实时聊天和互传信息，大部分还集成了语音聊天、文件传输的功能。下面介绍即时通信软件的一些主要功能。

- 文件传输：高速、稳定的实时文件传输功能，支持断点续传，并且支持离线文件传输。
- 即时消息：联机与脱机消息，支持消息的自定义，支持多人对话和消息群发。
- 视频功能：可自定义图像的压缩级别，以适应各种上网速度的要求。

- 群组功能：支持百人群组，且群组模式下支持自定义表情及贴图功能。
- 远程协助：对方能清晰地看到本地操作，协助更到位、更快捷。
- 电子名片：用户可设置个人电子名片，便于商务交流信息的宣传。
- 网络硬盘：具有分享、保存和提取文件功能，不占用磁盘空间。
- 语音对话：采用成熟的语音压缩技术，通话双方可得到很好的通话效果。
- 状态管理：有离开、忙碌、会议等常用状态，还提供自定义在线状态的功能。
- 界面更换：支持界面“皮肤”的更换，用户可自由选择。
- 自助广告：支持客户端的广告内容的设定，便于与商务网站的整合。
- Web 标签：支持自设客户端 Web 标签，支持动态参数，方便与其他 Web 整合。
- 网站融合：能与网站良好地融合，实现单机在线图标即能沟通。
- 升级：客户端用户可以进行相应的文件更新。

下面介绍几种当前国内外比较流行的即时通信软件。

1. ICQ

ICQ 作为 IM 软件领域的缔造者，不得不说它成就了一段辉煌历史。1996 年 7 月成立的 Mirabilis 公司于同年 11 月推出了全世界第一款即时通信软件 ICQ（目前 ICQ 已经归 AOL 旗下所有），取意为“我在找你”——“I Seek You”，简称 ICQ。

这款软件一经推出，即刻全球响应，凭借着前所未有的创意很快在全世界拥有了大批的用户，即使在当时互联网不太发达的亚洲，市场用户量也占到了 70%，在国内更是占到了 80%。但是到了现在，根据调查显示，国内的 IM 软件排名中 ICQ 已大大落后，不能满足中文用户的使用习惯是影响中国市场占有率的一个重要因素。

2. QQ

QQ 是 1999 年 2 月由腾讯自主开发的基于 Internet 的即时通信网络工具——腾讯即时通信（Tencent Instant Messenger，简称 TM 或腾讯 QQ），其合理的设计、良好的易用性、强大的功能，稳定高效的系统运行，赢得了用户的青睐；QQ 以前是模仿 ICQ 来的，ICQ 是国际的一个聊天工具，OICQ 模仿它在 ICQ 前加了一个字母 O，意思是“开放的 ICQ”，后因版权问题改名为 QQ。

QQ 不仅仅是简单的即时通信软件，它与全国多家寻呼台、移动通信公司合作，实现传统的无线寻呼网、GSM 移动电话的短消息互连，是国内最为流行功能最强的即时通信（IM）软件。腾讯 QQ 支持在线聊天、即时传送视频、语音、文件等多种多样的功能。同时，QQ 还可以与移动通信终端、IP 电话网、无线寻呼等多种通信方式相连，使 QQ 不仅仅是单纯意义的网络虚拟呼机，而是一种方便、实用、超高效的即时通信工具。

随着时间的推移，根据 QQ 所开发的附加产品越来越多，如 QQ 宠物、QQ 音乐、QQ 空间、QQ 游戏等，受到 QQ 用户的青睐。

3. MSN

MSN Messenger 是出自微软公司的即时通信工具，和腾讯 QQ 属同一个类别的工具。

MSN 是四大顶级个人即时通信工具之一，在国内通信工具市场上稳稳占据第二的位置，仅次于腾讯 QQ。

MSN 全称为 Microsoft Service Network（微软网络服务），MSN Messenger 的最新版本是 Windows Live Messenger 9.0。“MSN Messenger”这个字眼相当含糊，因为微软公司用这个术语关系了几个不同部分的消息解决方案。通过“MSN Messenger 网络”聊天，用来连接 MSN Messenger 网络的最流行的程序是 MSN Messenger，而程序在 MSN Messenger 网络中使用的语言则是“MSN Messenger 协议”。MSN 作为一种联络通信工具，已经越来越普及了，特别是在上班族中。MSN（MicroSoft Network）是微软公司提供的 Internet 服务，也就是说，与网络同步服务（initially meant to be a parallel net to the Internet）。

4.6.2　最新的网络交流工具

1．微博

微博，即微博客（MicroBlog）的简称，是一个基于用户关系的信息分享、传播以及获取平台，用户可以通过 Web、WAP 以及各种客户端组建个人社区，以 140 字左右的文字更新信息，并实现即时分享。最早也是最著名的微博是美国的 twitter，根据相关公开数据，截至 2010 年 1 月份，该产品在全球已经拥有 7500 万注册用户。2009 年 8 月份中国最大的门户网站新浪网推出“新浪微博”内测版，成为门户网站中第一家提供微博服务的网站，微博正式进入中文上网主流人群视野。2012 年 10 月，有报告显示至 2011 年 12 月，中国微博用户总数达到 2.498 亿。

微博是一种通过关注机制分享简短实时信息的广播式的社交网络平台，其中有 5 个方面的理解。

- 关注机制：可单向可双向两种；
- 简短内容：通常为 140 个字；
- 实时信息：最新实时信息；
- 广播式：公开的信息，谁都可以浏览；
- 社交网络平台：把微博归为社交网络。

微博提供这样一个平台，既可以作为观众，在微博上浏览感兴趣的信息；也可以作为发布者，在微博上发布内容供别人浏览。发布的内容一般较短，有 140 字的限制，微博由此得名。微博也可以发布图片、分享视频等。微博最大的特点就是发布信息快速，信息传播的速度快。例如，有 200 万听众，发布的信息会在瞬间传播给 200 万人。首先，相对于强调版面布置的博客来说，微博的内容组成只是由简单的只言片语组成，从这个角度来说，对用户的技术要求门槛很低，而且在语言的编排组织上，没有博客那么高。其次，微博开通的多种应用程序接口（API）使得大量的用户可以通过手机、网络等方式来即时更新自己的个人信息。

2．微信

微信是腾讯公司于 2011 年 1 月 21 日推出的一款通过网络快速发送语音短信、视频、

图片和文字，支持多人群聊的手机聊天软件。用户可以通过微信与好友进行形式上更加丰富的类似于短信、彩信等方式的联系。微信软件本身完全免费，使用任何功能都不会收取费用，微信时产生的上网流量费由网络运营商收取。2012 年 9 月 17 日，微信注册用户超过 2 亿。

微信是一种更快速的即时通信工具，具有零资费、跨平台沟通、显示实时输入状态等功能，与传统的短信沟通方式相比，更灵活、智能，且节省资费。

微信主要是用于手机聊天的软件，支持智能手机中的 iOS、Android、Windows Phone 和塞班平台。具体特点如下：

- 支持发送语音短信、视频、图片（包括表情）和文字；
- 支持多人群聊（最高 20 人。100 人 200 人群聊正在内测）；
- 支持查看所在位置附近使用微信的人（LBS 功能）；
- 支持腾讯微博、QQ 邮箱、漂流瓶、语音记事本、QQ 同步助手等插件功能。

3. FACETIME

几十年来，人们一直梦想能够使用可视电话。现在，iPhone 4 令梦想成真。通过 WLAN，连接任意两部支持 Facetime 的设备（目前有 MacBook、iPhone 4、iPhone 4S、iPhone 5、iPod touch 4、iPod touch 5、iPad 2、The new iPad、iPad 4 和 iPad mini），只要轻点一下按钮，就可以与地球另一端的人相视微笑，或与好友分享故事并看着他开心大笑。

实验 11　DNS 服务器配置

一、实验说明

DNS 服务器提供域名服务，可实现 IP 地址和域名之间的转换。通常人们使用容易记忆的域名来访问站点，但网络传输使用的是 IP 地址，因此，要想用域名来访问站点，需要先配置 DNS 服务器。

二、实验目的

（1）掌握在 Windows 上进行 DNS 服务器配置的方法。
（2）加深对客户机/服务器模式的理解。
（3）熟悉服务器配置向导的使用方法。

三、实验内容

（1）安装 DNS 服务器。
（2）创建区域。
（3）创建域名。
（4）设置 DNS 客户端。
（5）删除 DNS 服务器。

四、实验准备

安装有 Windows 2008 Server 并连接在网络中的计算机。

五、实验参考步骤

1. 安装 DNS 服务器

在默认情况下，安装 Windows Server 系统时并不包括安装 DNS 服务器。安装 DNS 服务器的基本过程如下。

① 依次选择“开始”→“管理工具”→“服务器管理器”选项，打开“服务器管理器”窗口。在该窗口中单击“角色”选项，然后单击“添加角色”，弹出“添加角色向导”对话框。在该对话框中找到“DNS 服务器”复选框，选中后单击“下一步”按钮，如图 4.15 所示。



图 4.15 “添加角色向导”窗口一

② 根据“添加角色向导”的提示，连续单击“下一步”按钮，最后单击“安装”按钮，如图 4.16 所示。

③ 等待一段时间后，安装成功。

2. 创建区域

创建一个 DNS 服务器，除了必需的计算机硬件、服务器软件外，还需要一个数据

库——一个新的区域来存储供局部用的 DNS 名称与 IP 地址或有关服务数据。因此，选定了主机之后，就要创建一个新的区域。创建一个新区域的过程如下。

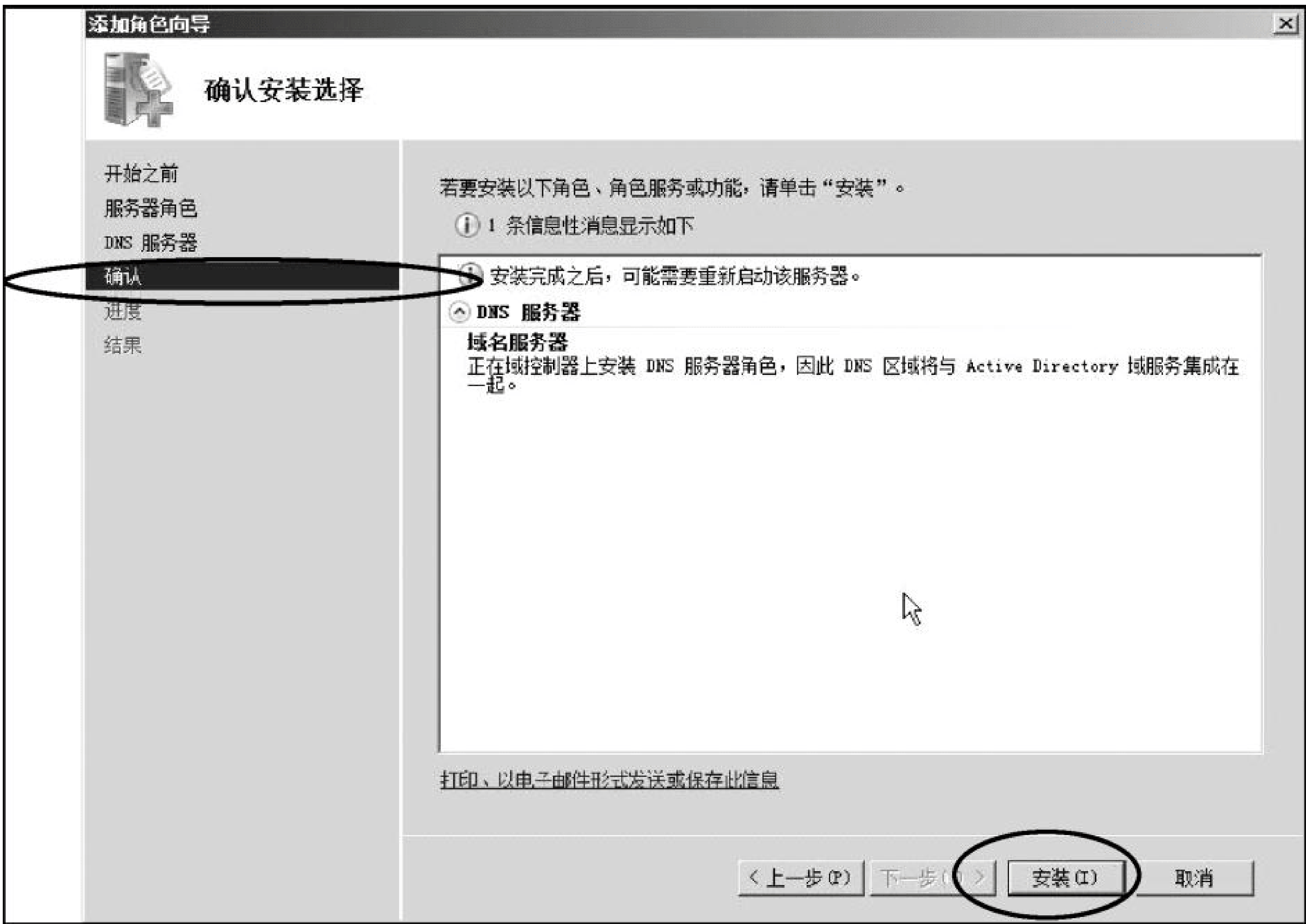


图 4.16 “添加角色向导”窗口二

1）创建正向查找区域

① 依次选择“开始”→“管理工具”→DNS 选项，打开“DNS 管理器”窗口，右击“正向查找区域”选项，选择“新建区域”命令，如图 4.17 所示。



图 4.17 新建区域

② 打开“区域类型”对话框，如图 4.18 所示。在“选择您要创建的区域的类型”选项组中有 3 个选项：“主要区域”、“辅助区域”和“存根区域”。用户可以根据区域存储和复

制的方式选择一个区域类型。这里选择“主要区域”。

③ 单击“下一步”按钮，在“区域名称”对话框中依照规范为新区域命名，这里命名为 test.com，如图 4.19 所示。

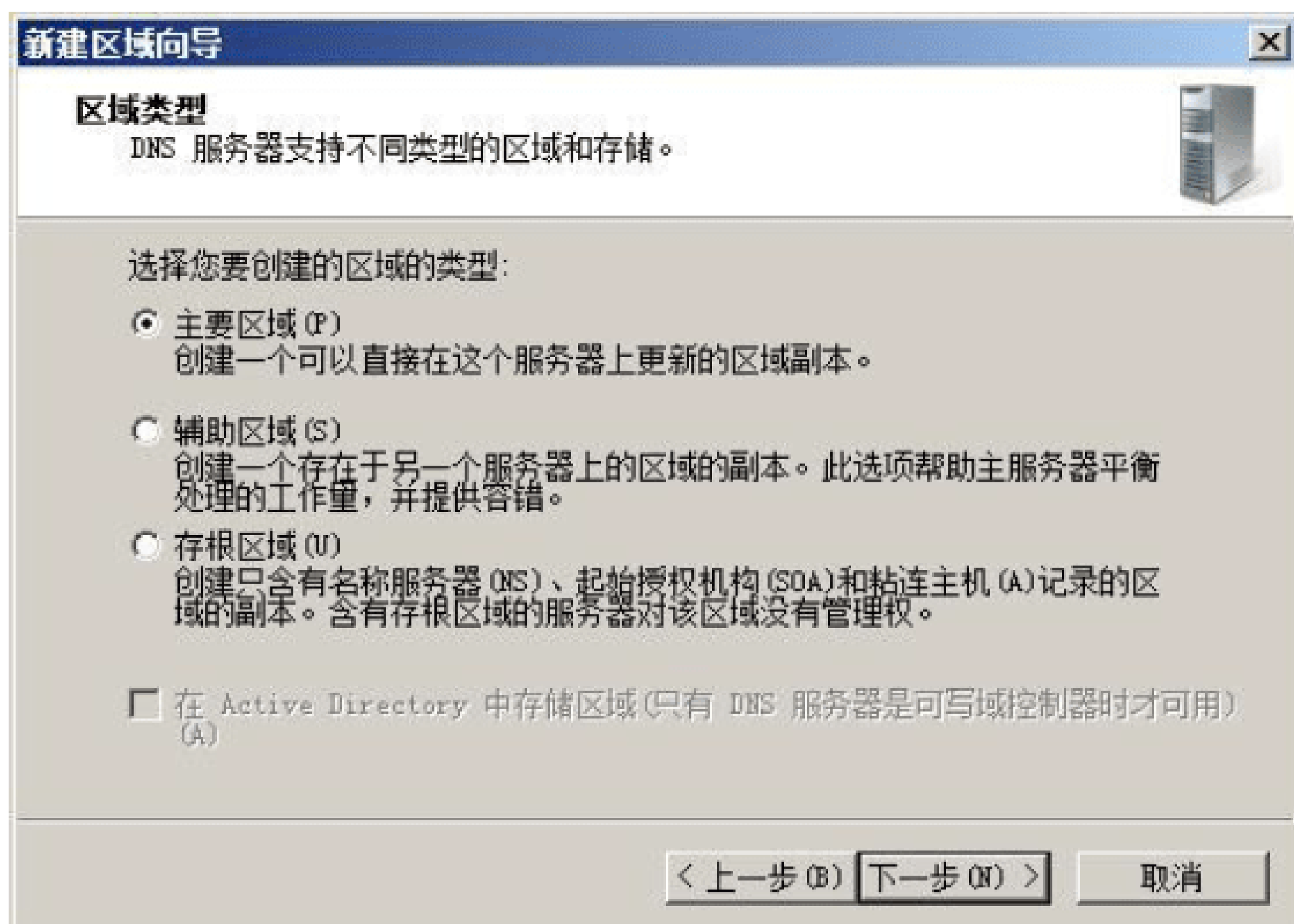


图 4.18　选择区域类型



图 4.19　填写区域名称

④ 单击“下一步”按钮，在“区域文件”对话框中可以选择“创建新文件”或“使用此现存文件”单选按钮。这里选择“创建新文件”，文件名为默认，如图 4.20 所示。

⑤ 单击“下一步”按钮，弹出“动态更新”对话框，用户可以选择“允许非安全和安全动态更新”或“不允许动态更新”单选按钮。这里选择“不允许动态更新”，如图 4.21 所示。

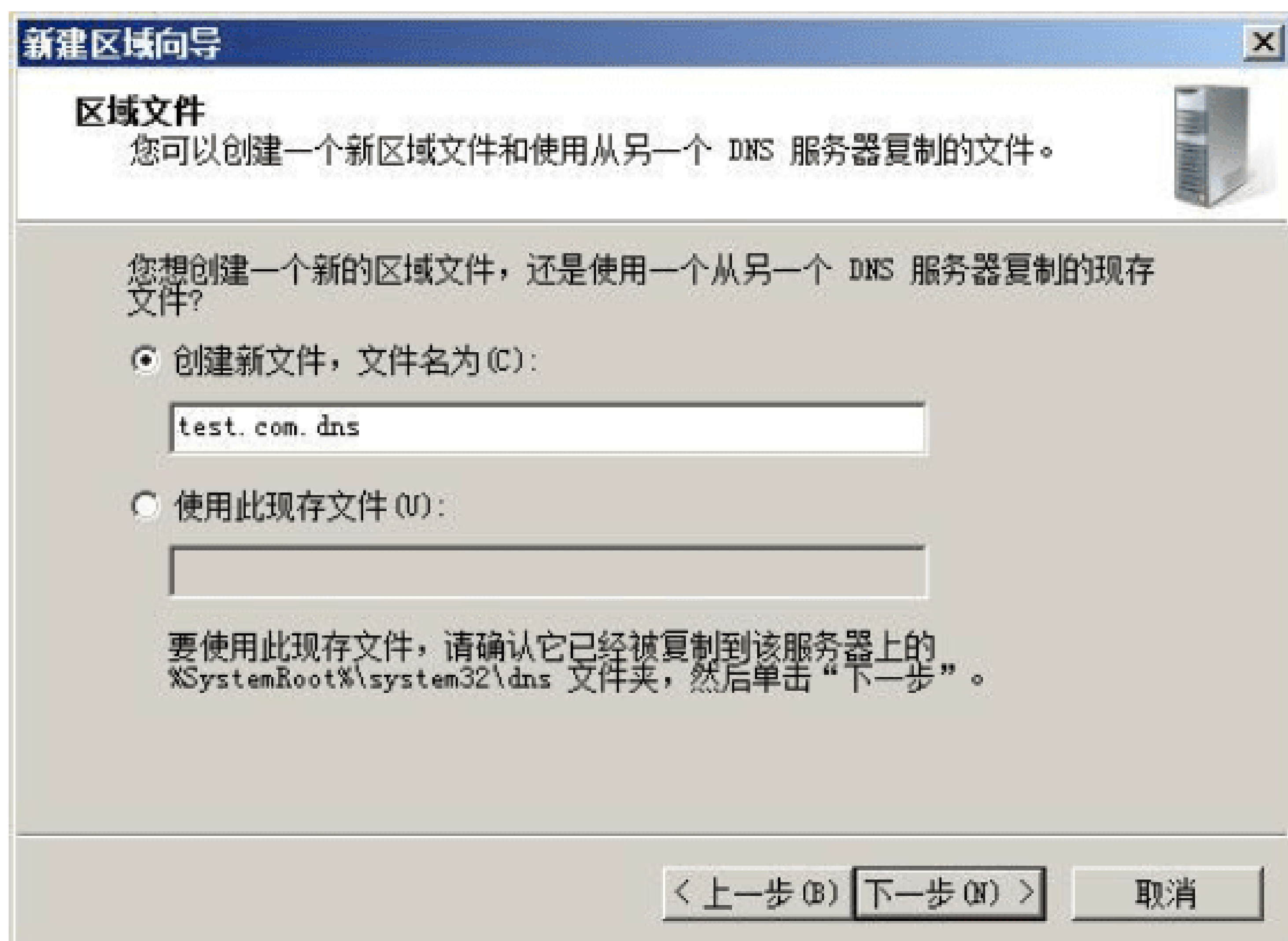


图 4.20　选择区域文件

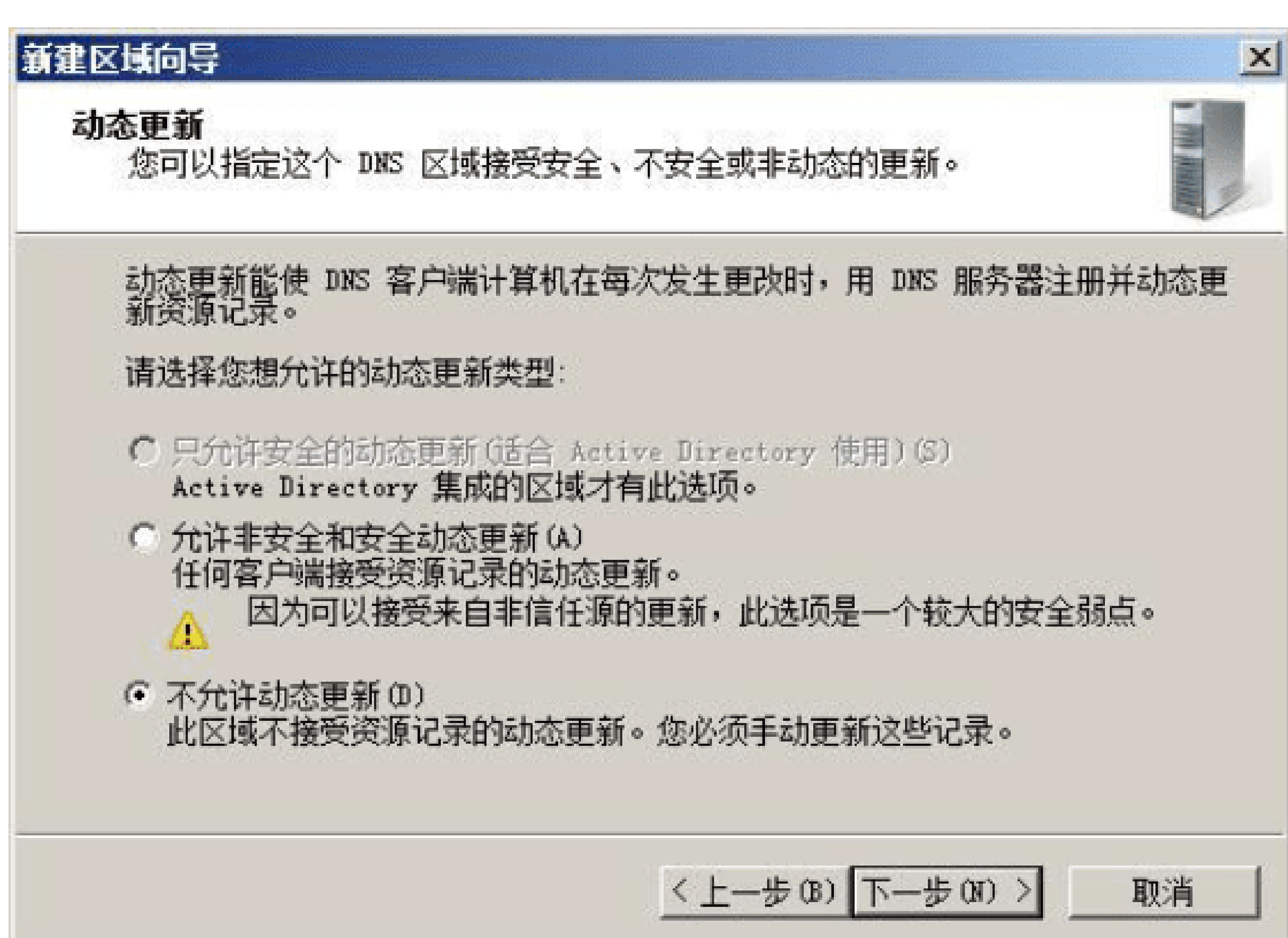


图 4.21　动态更新选项

⑥ 单击“下一步”按钮，再单击“完成”按钮，完成正向搜索区域下的新建区域的配置。

2）创建反向查找区域

① 右击“反向查找区域”选项，选择“新建区域”命令，如图 4.22 所示。

② 打开“区域类型”对话框，如图 4.23 所示。在“选择您要创建的区域的类型”选项组中有 3 个选项：“主要区域”“辅助区域”和“存根区域”。用户可以根据区域存储和复制的方式选择一个区域类型。这里选择“主要区域”。

③ 单击“下一步”按钮，选择“IPv4 反向查找区域”单选按钮，如图 4.24 所示。如果所用 IP 为 IPv6 地址，则选择“IPv6 反向查找区域”单选按钮。



图 4.22　创建反向查找区域

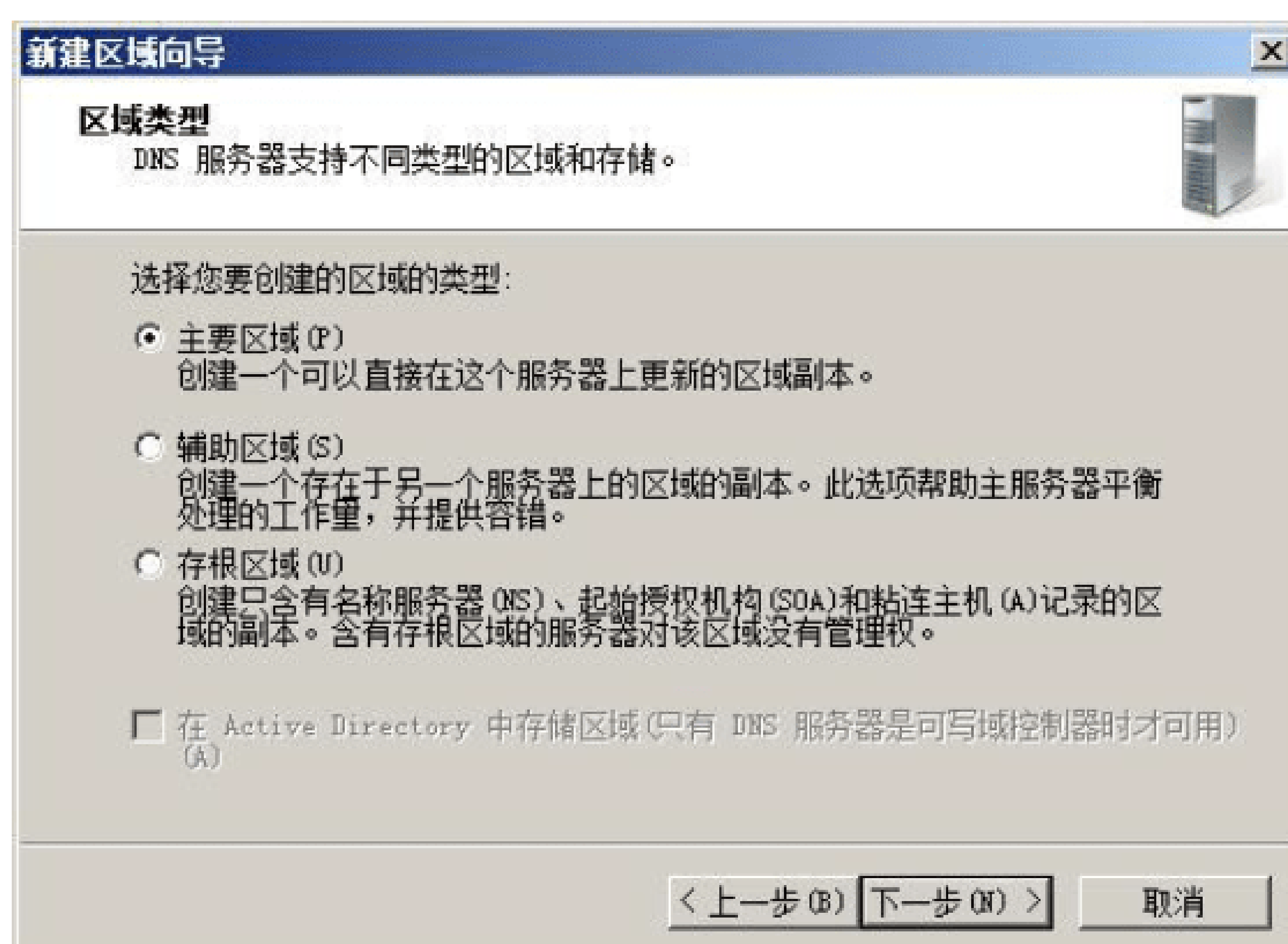


图 4.23　选择反向区域类型

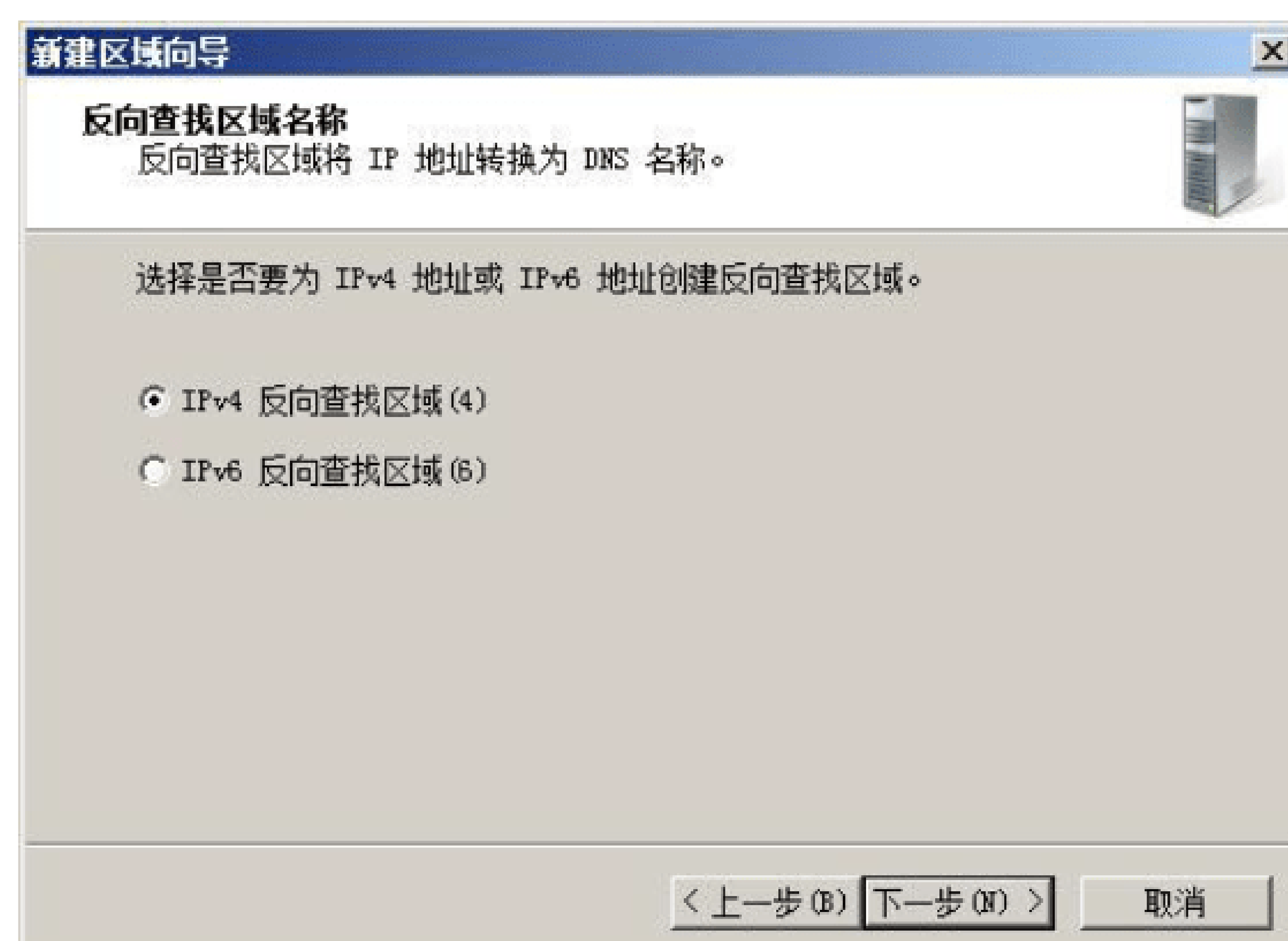


图 4.24　为 IPv4 或 IPv6 创建反向查找区域

④ 单击“下一步”按钮，输入“网络 ID”。这里输入 172.16.18，如图 4.25 所示。

⑤ 单击“下一步”按钮，在“区域文件”对话框中可以选择“创建新文件”或“使用此现存文件”单选按钮。这里选择“创建新文件”，文件名为默认，如图 4.26 所示。

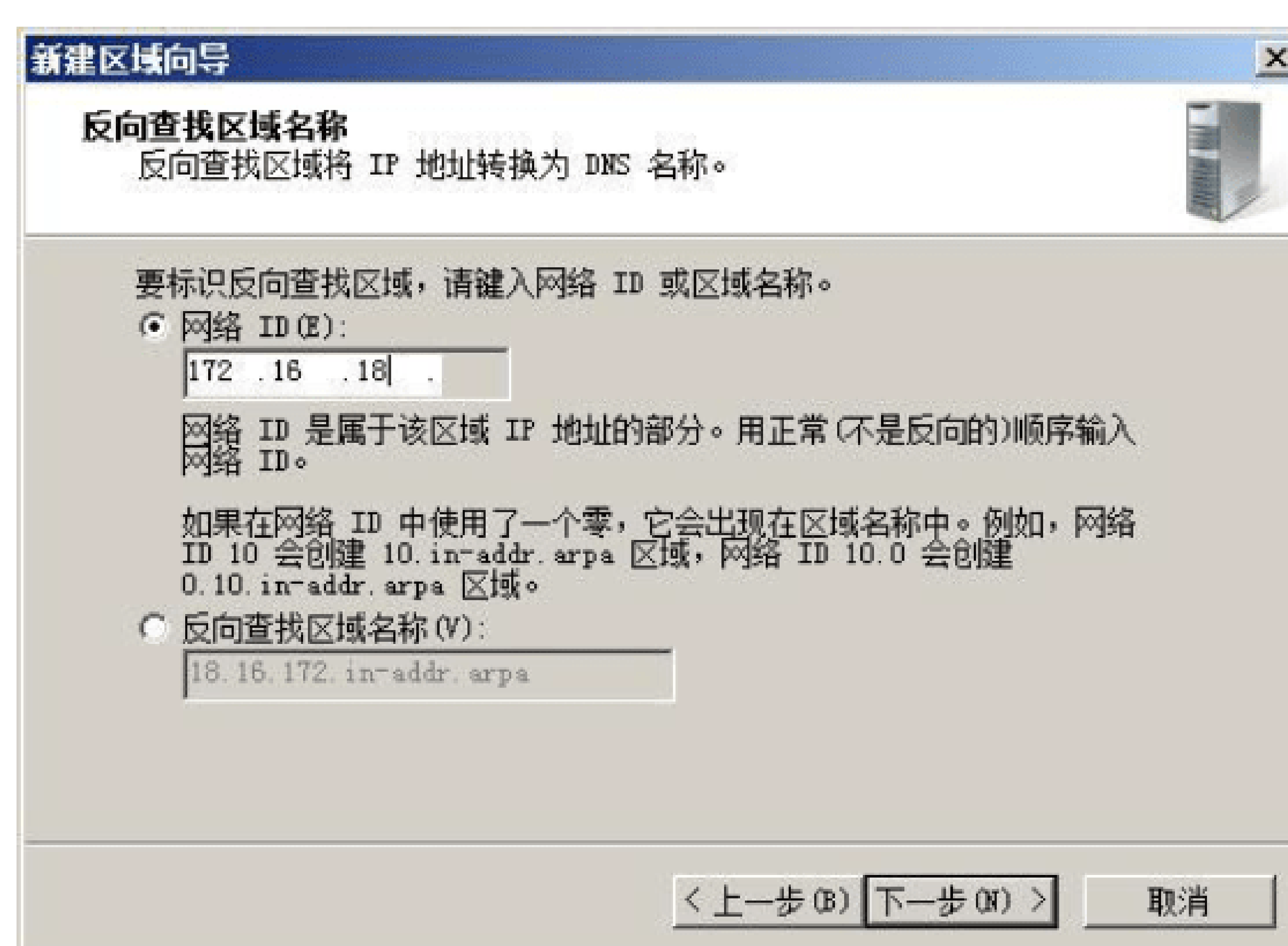


图 4.25　设置网络 ID

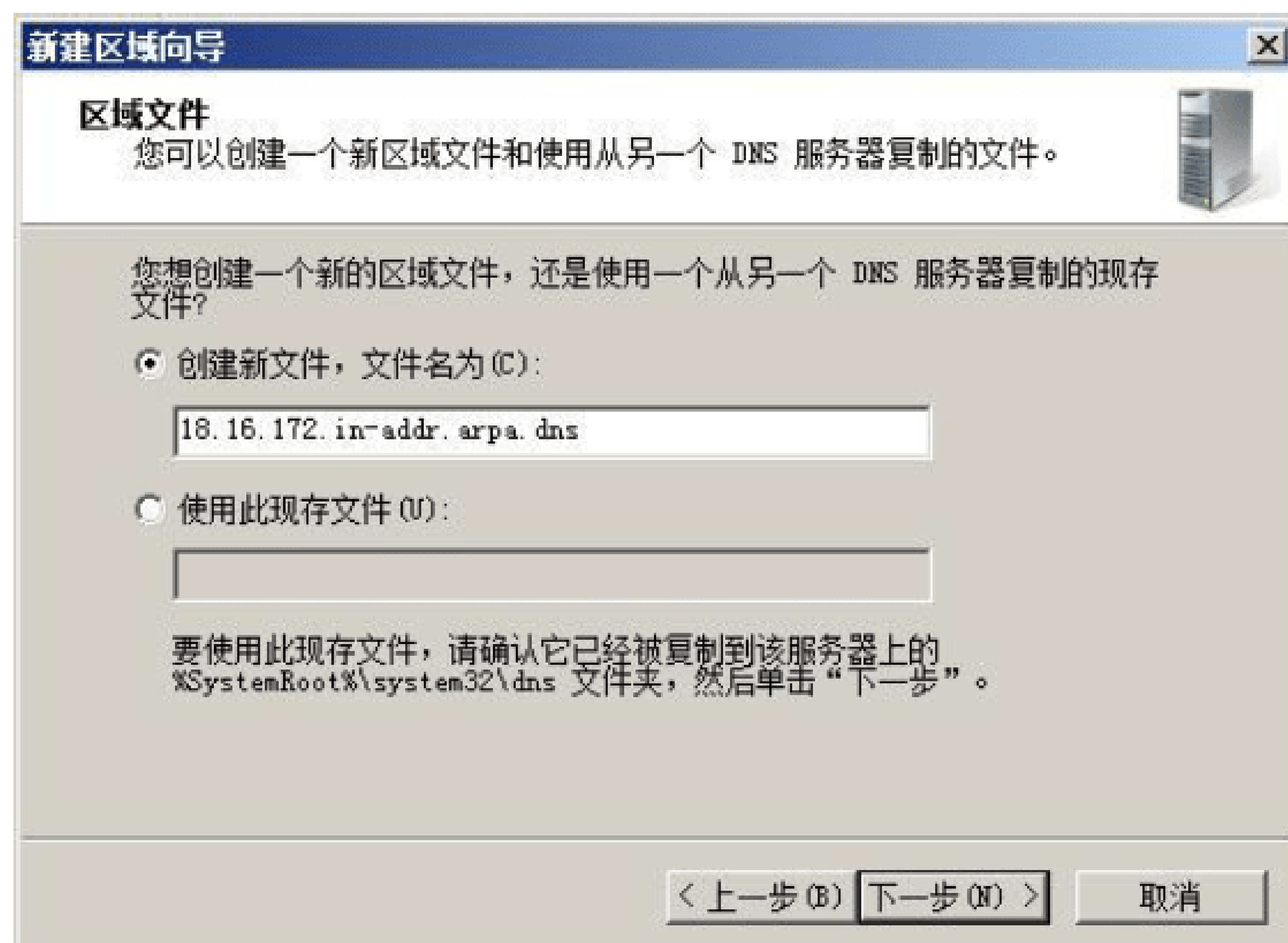


图 4.26　创建区域文件

⑥ 单击“下一步”按钮，弹出“动态更新”对话框，用户可以选择“允许非安全和安全动态更新”或“不允许动态更新”单选按钮。这里选择“不允许动态更新”，如图 4.27 所示。

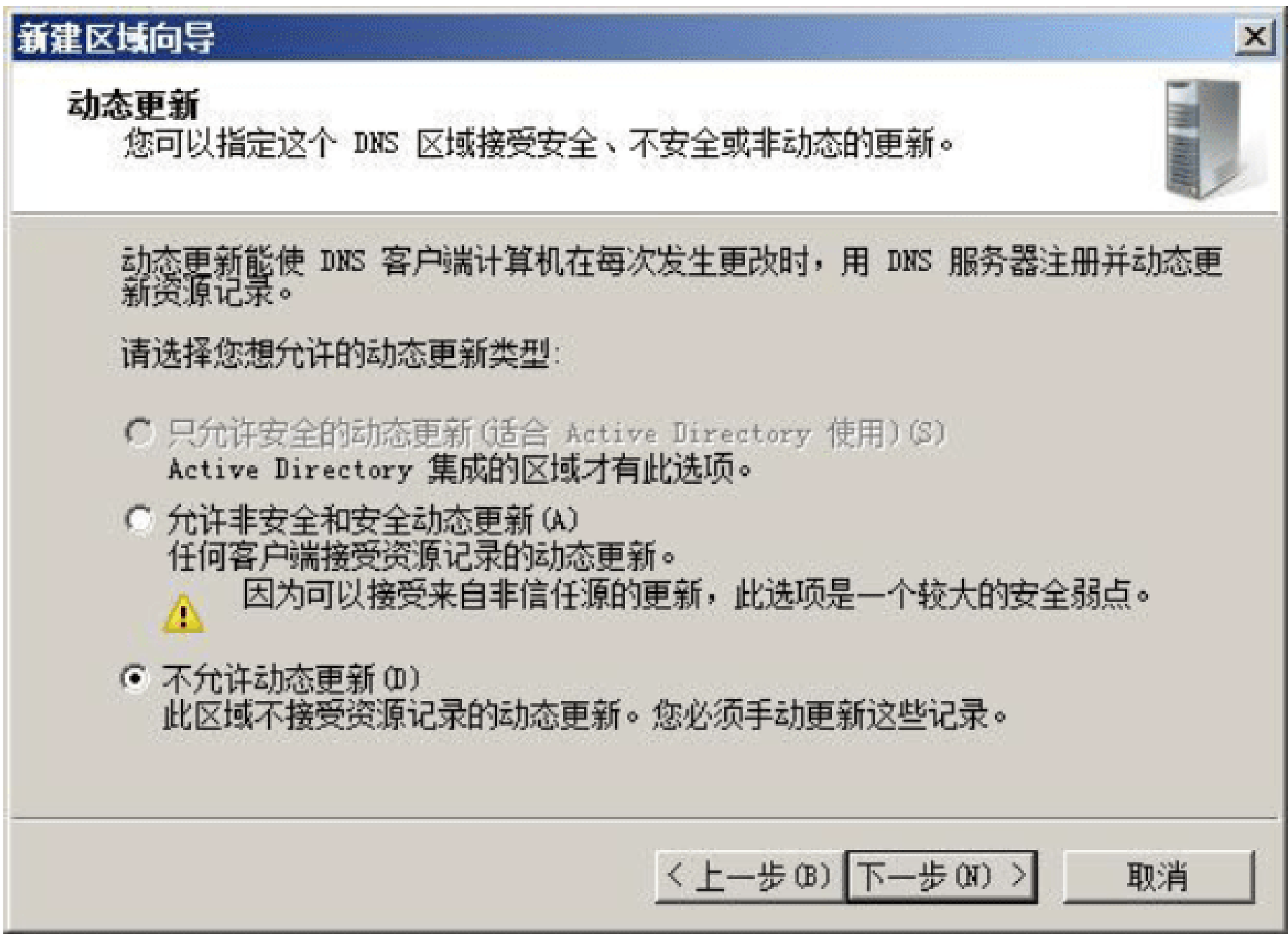


图 4.27　动态更新选项

⑦ 单击“下一步”按钮，再单击“完成”按钮，完成反向搜索区域下的新建区域的配置。

3）创建主机

① 右击“test.com”选项，选择“新建主机”命令，如图 4.28 所示。

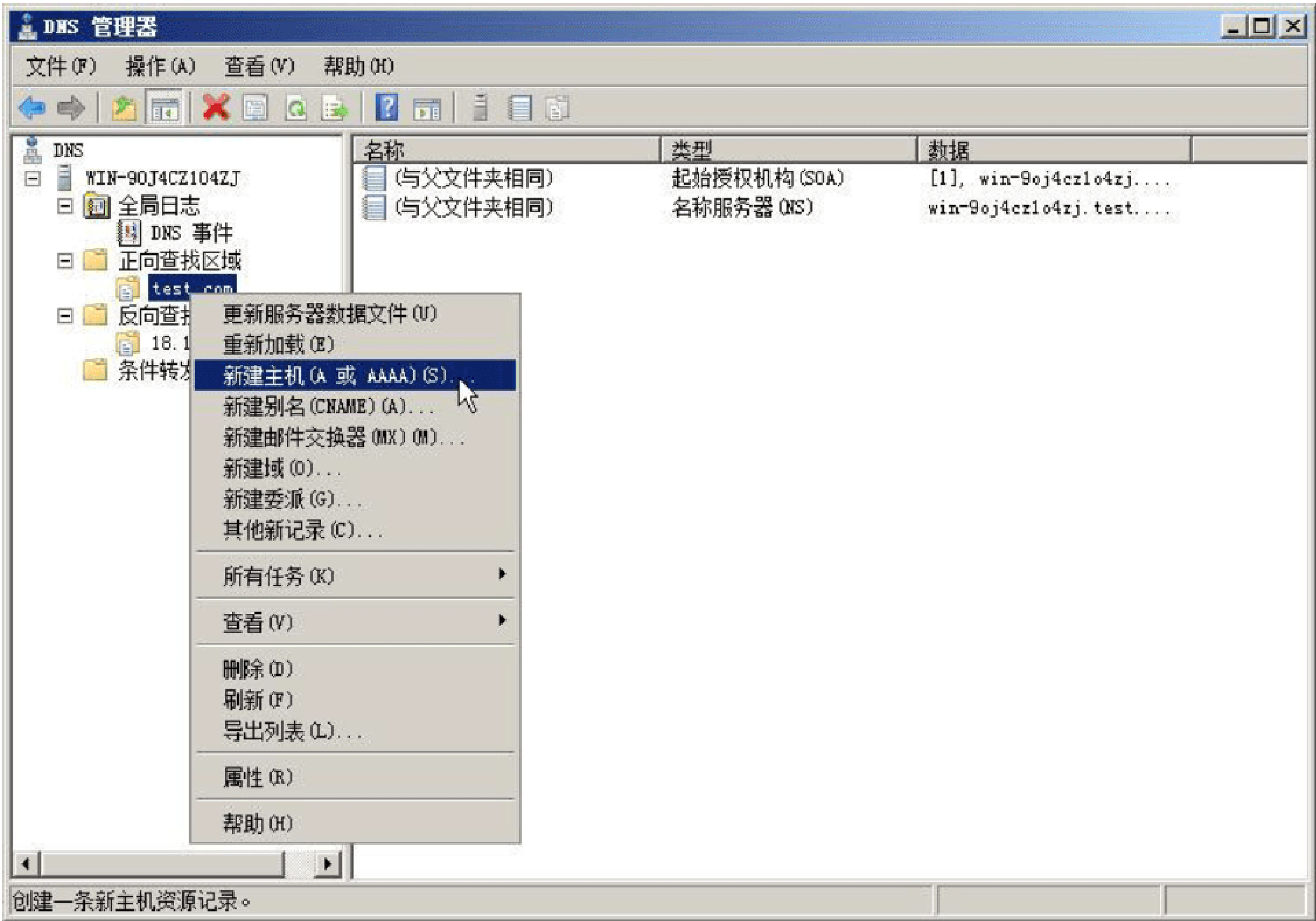


图 4.28　创建主机

② 弹出“新建主机”对话框，在“名称”文本框中输入主机名为 www。这里输入可

以标识主机意义的名称，在“IP 地址”文本框中输入 172.16.18.76（本计算机的 IP 地址），如图 4.29 所示。如果选中“创建相关的指针记录”复选框，则在反向区域中自动创建一条指针记录；如果不选中，则手工在反向区域中创建一条指针记录。这里不选中（要想自动在反向区域创建一条指针记录，那么在选中“创建相关的指针记录”的同时，反向查找区域必须已经创建）。

③ 单击“添加主机”按钮，弹出成功创建主机记录窗口，主机创建完成，如图 4.30 所示。



图 4.29 新建主机名称和 IP 地址



图 4.30 成功创建主机记录对话框

4）创建指针记录

① 右击“test.com 反向区域”选项，选择“新建指针”命令，如图 4.31 所示。

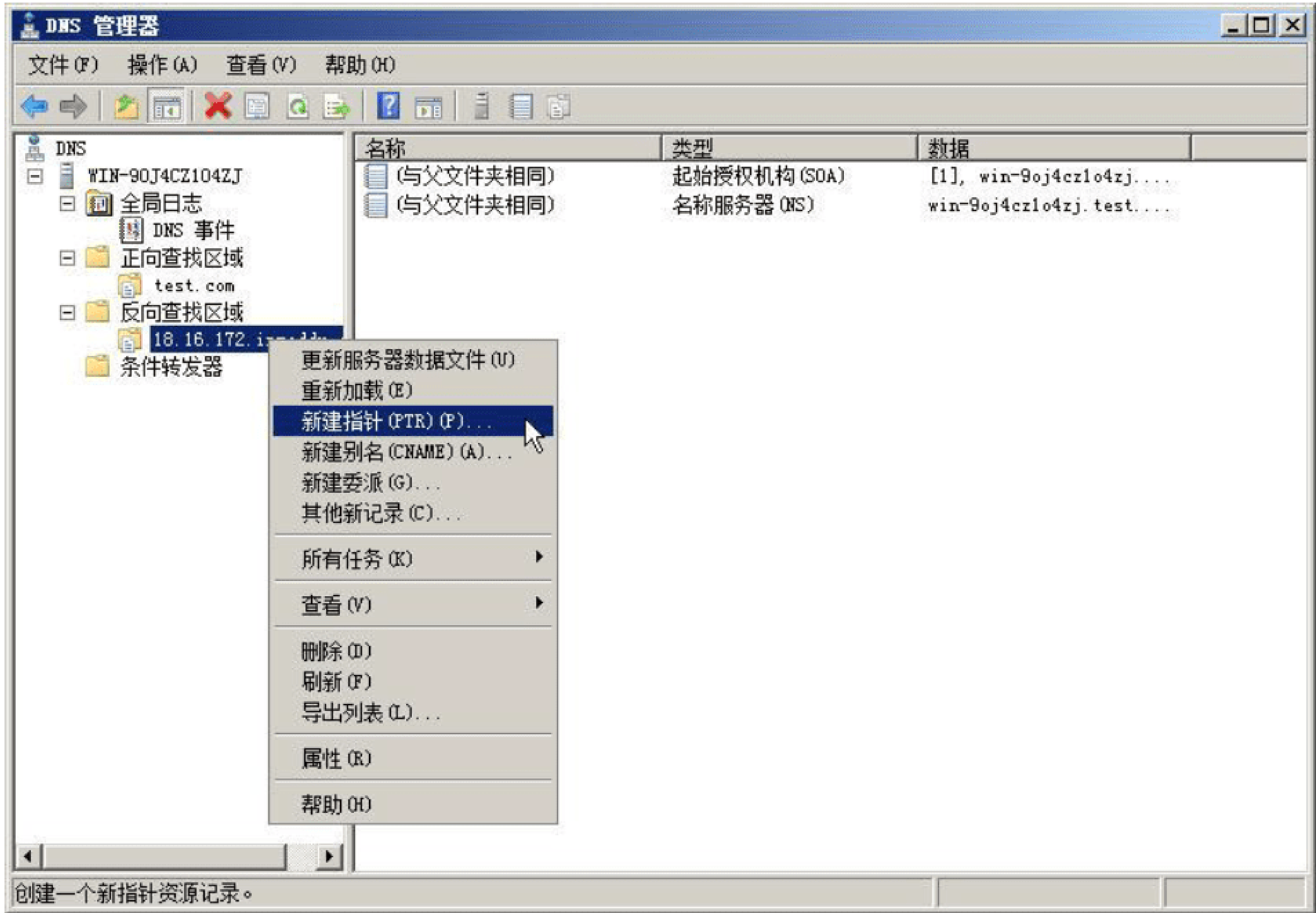


图 4.31 创建指针

② 弹出“新建指针”对话框，输入主机 IP 地址为 172.16.18.76，单击“浏览”按钮，添加主机名，如图 4.32 所示。

③ 单击“确定”按钮，完成指针的创建。

3. 验证 DNS 服务器

1）设置 DNS 客户端

在客户机“Internet 协议版本 4（TCP/IPv4）属性”对话框中的“首选 DNS 服务器”编辑框中设置刚刚部署的 DNS 服务器的 IP 地址（本例为 172.16.18.76），如图 4.33 所示。

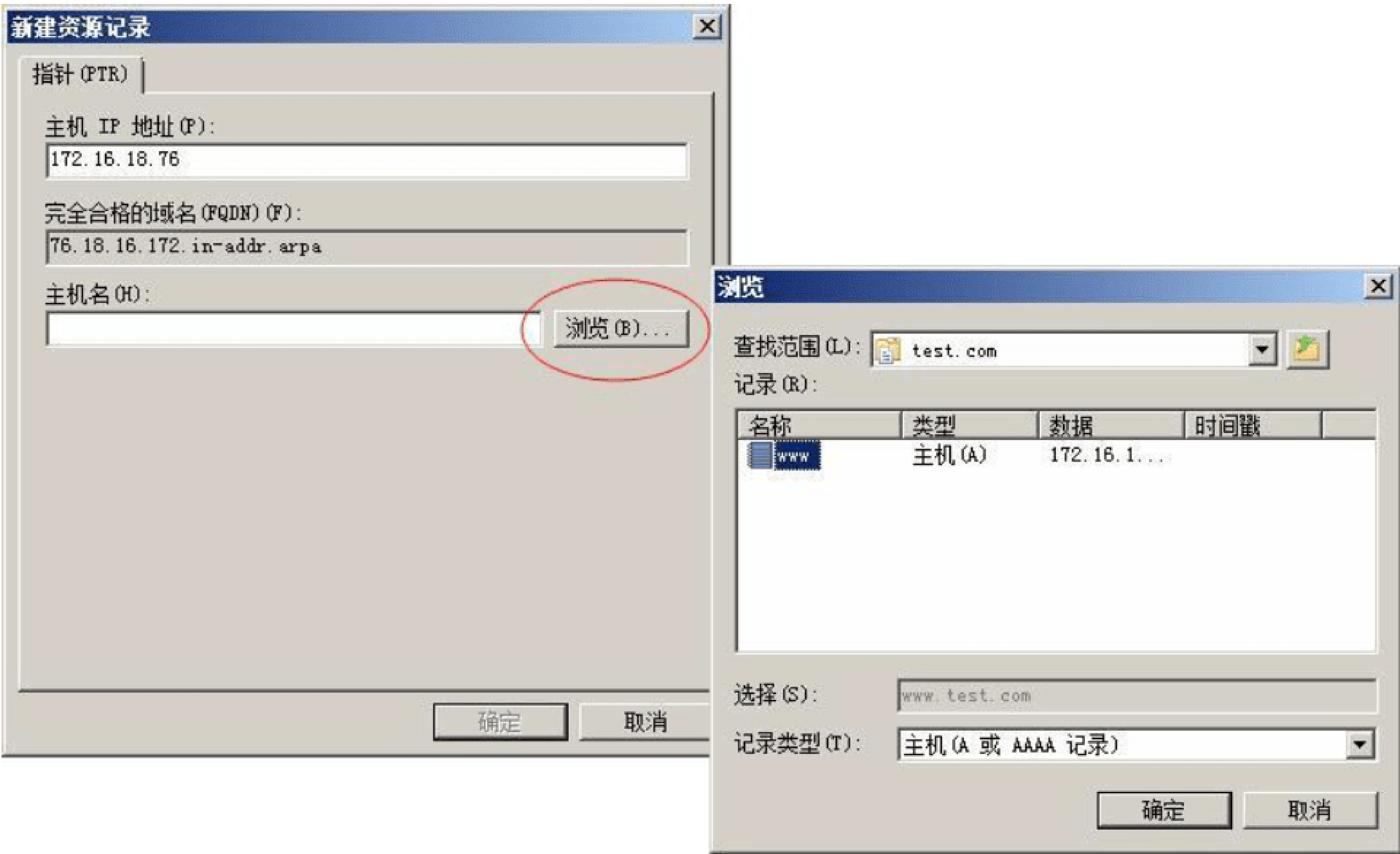


图 4.32 输入指针记录的 IP 地址和主机名

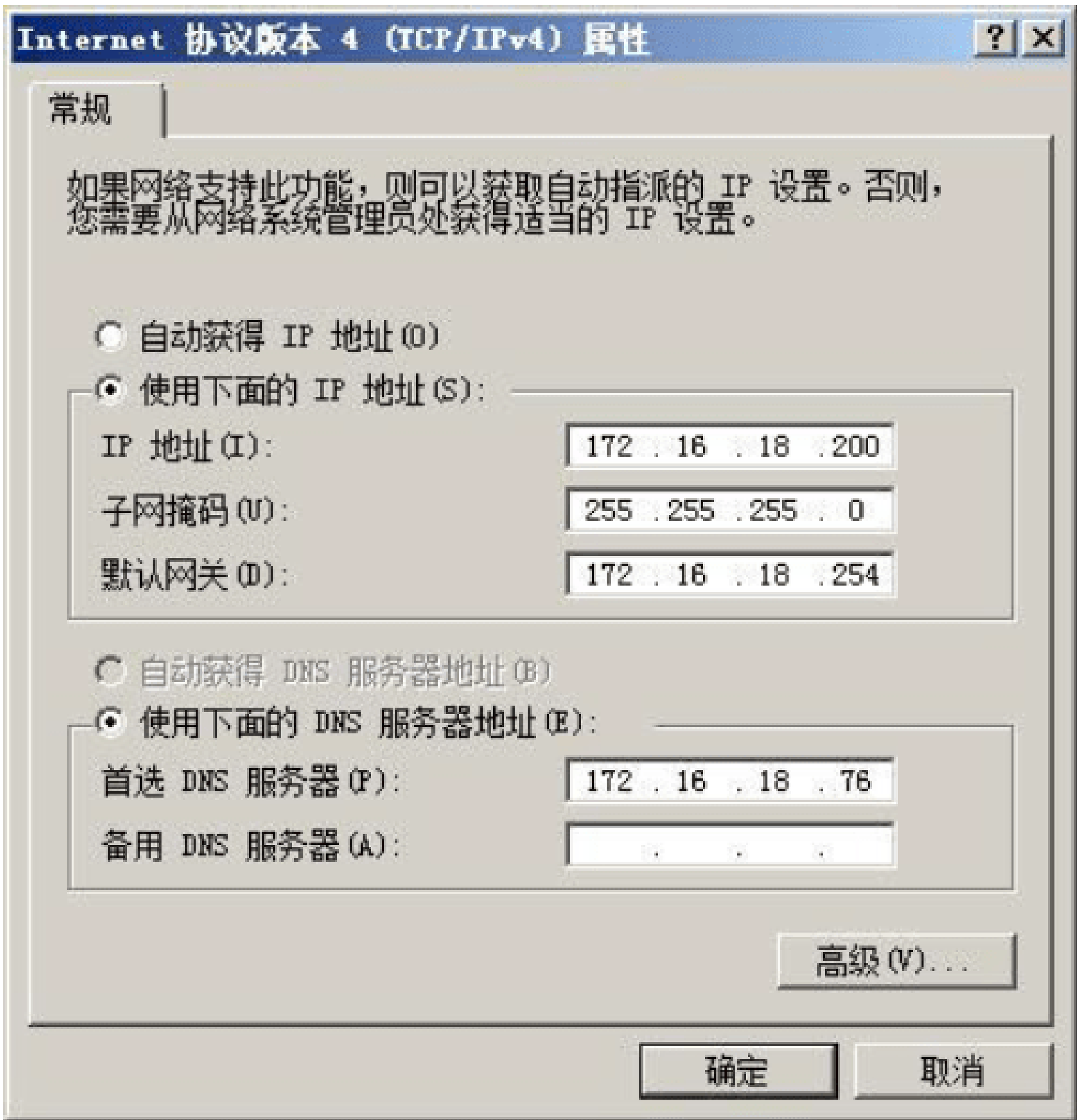


图 4.33 设置客户端 DNS 服务器地址

2）用 nslookup 命令验证

打开“命令提示符”界面，输入 nslookup www.test.com 测试。

4. 删除 DNS 服务器

配置好服务器的各项功能后，若遇到创建的 DNS 服务器不能正常运行的情况，需要将它删除以便创建新的 DNS 服务器。删除 DNS 服务器的方法是在如图 4.34 所示的“DNS 管理器”窗口中，右击服务器名称，选择“删除”命令，所选择服务器即可删除。

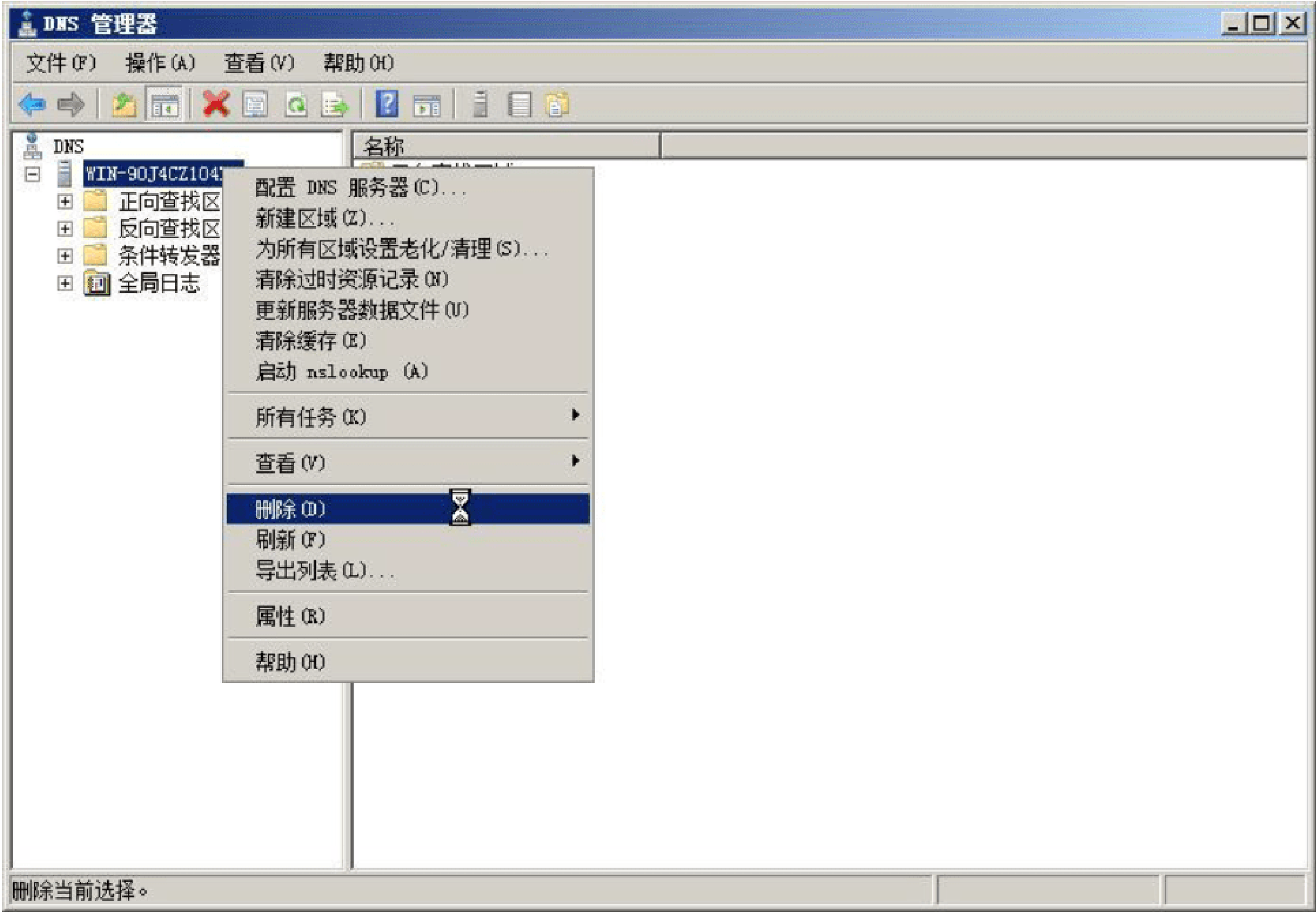


图 4.34 删除 DNS 服务器

六、附加实验

配置 DNS 服务器，实现多个域名解析。

七、分析与讨论

（1）安装 DNS 的服务器端与安装 DNS 的客户机端的作用各是什么？

（2）安装 DNS 的服务器端最关键的操作是什么？

实验 12　FTP 服务器配置

一、实验说明

FTP 服务器是在互联网上提供存储空间的计算机，它们依照 FTP 协议提供服务。FTP 的全称是 File Transfer Protocol（文件传输协议），即专门用来传输文件的协议。简单地说，支持 FTP 协议的服务器就是 FTP 服务器。

二、实验目的

（1）掌握在 Windows 上进行 FTP 服务器配置的方法。
（2）加深对客户机/服务器模式的理解。
（3）熟悉服务器配置向导的使用方法。

三、实验内容

（1）FTP 站点的规划。
（2）管理默认的 FTP 站点。
（3）添加新的 FTP 站点。
（4）FTP 站点的设置和访问。

四、实验准备

安装有 Windows Server 2008 并连接在网络中的计算机。

五、实验参考步骤

1. 添加 FTP 角色功能

选择安装 FTP 的角色服务，如图 4.35 所示。

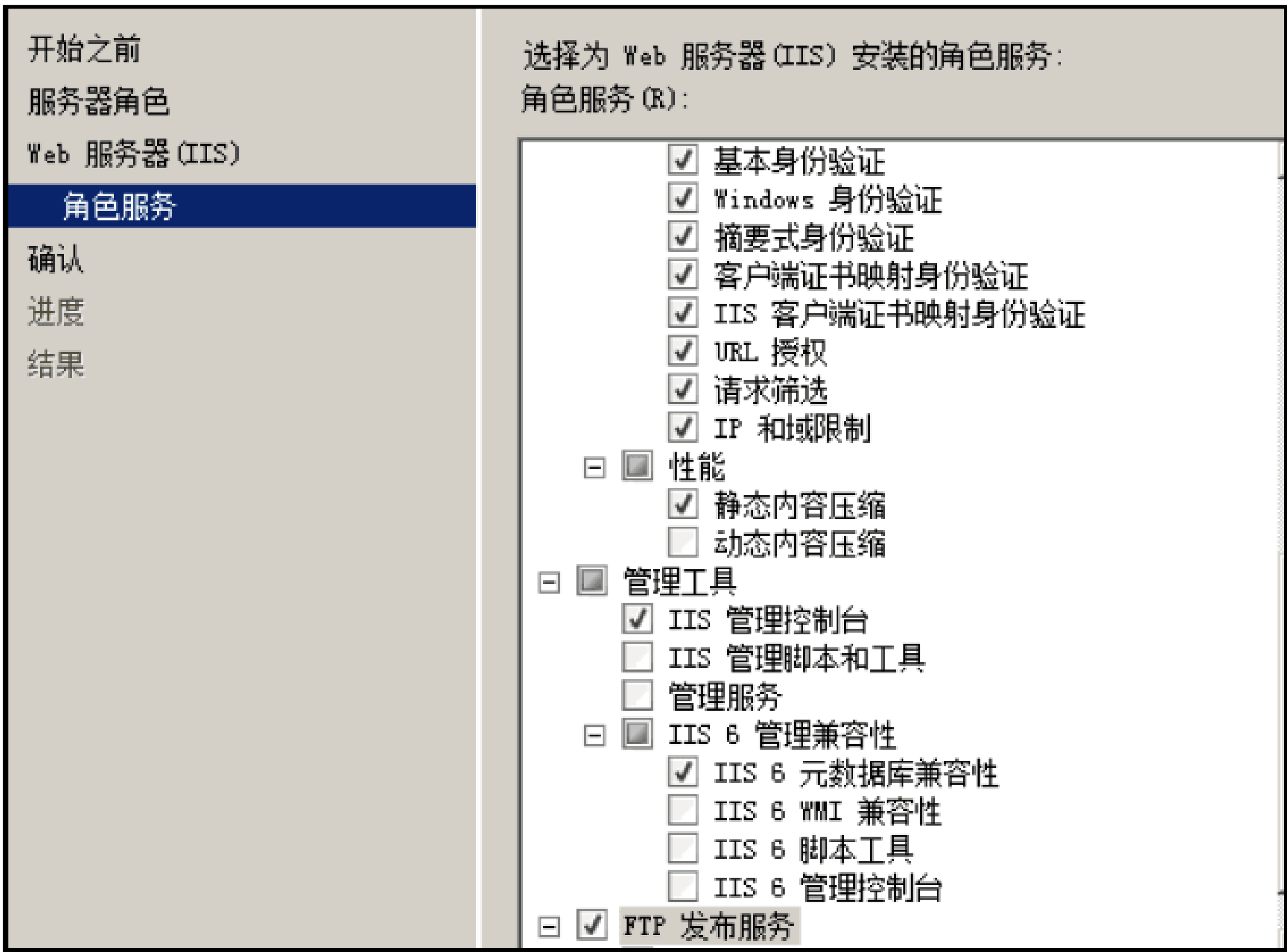


图 4.35　安装 FTP 角色服务

2. 配置默认 FTP 站点

① 打开默认 FTP 站点的属性对话框，如图 4.36 所示。

② 设置默认 FTP 站点的安全账户，取消选中“允许匿名连接”复选框，如图 4.37 所示。

③ 设置 FTP 站点的主目录路径，并设置用户在本目录下读取和写入的权限，如图 4.38 所示。

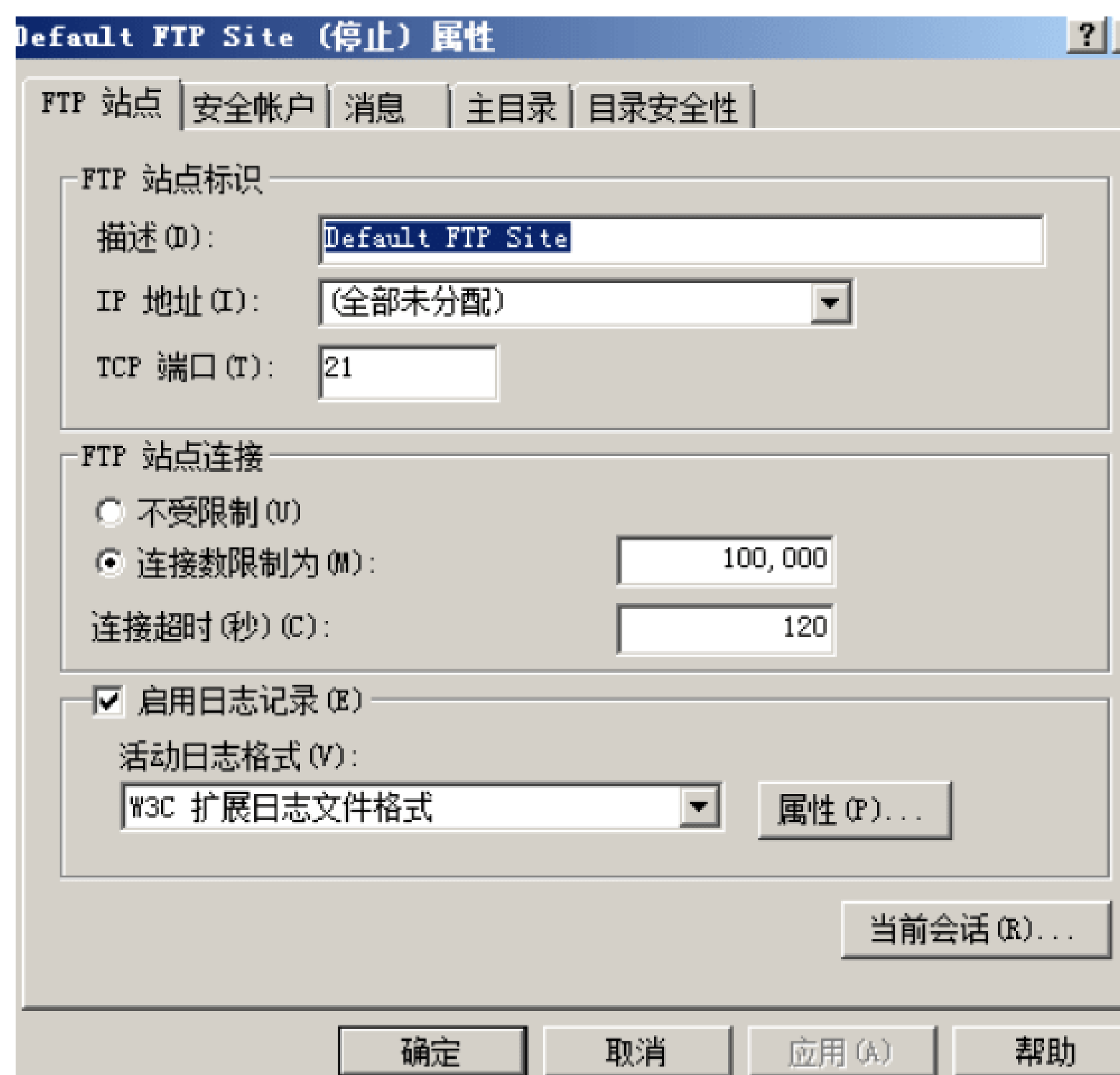


图 4.36　设置 FTP 站点的标识

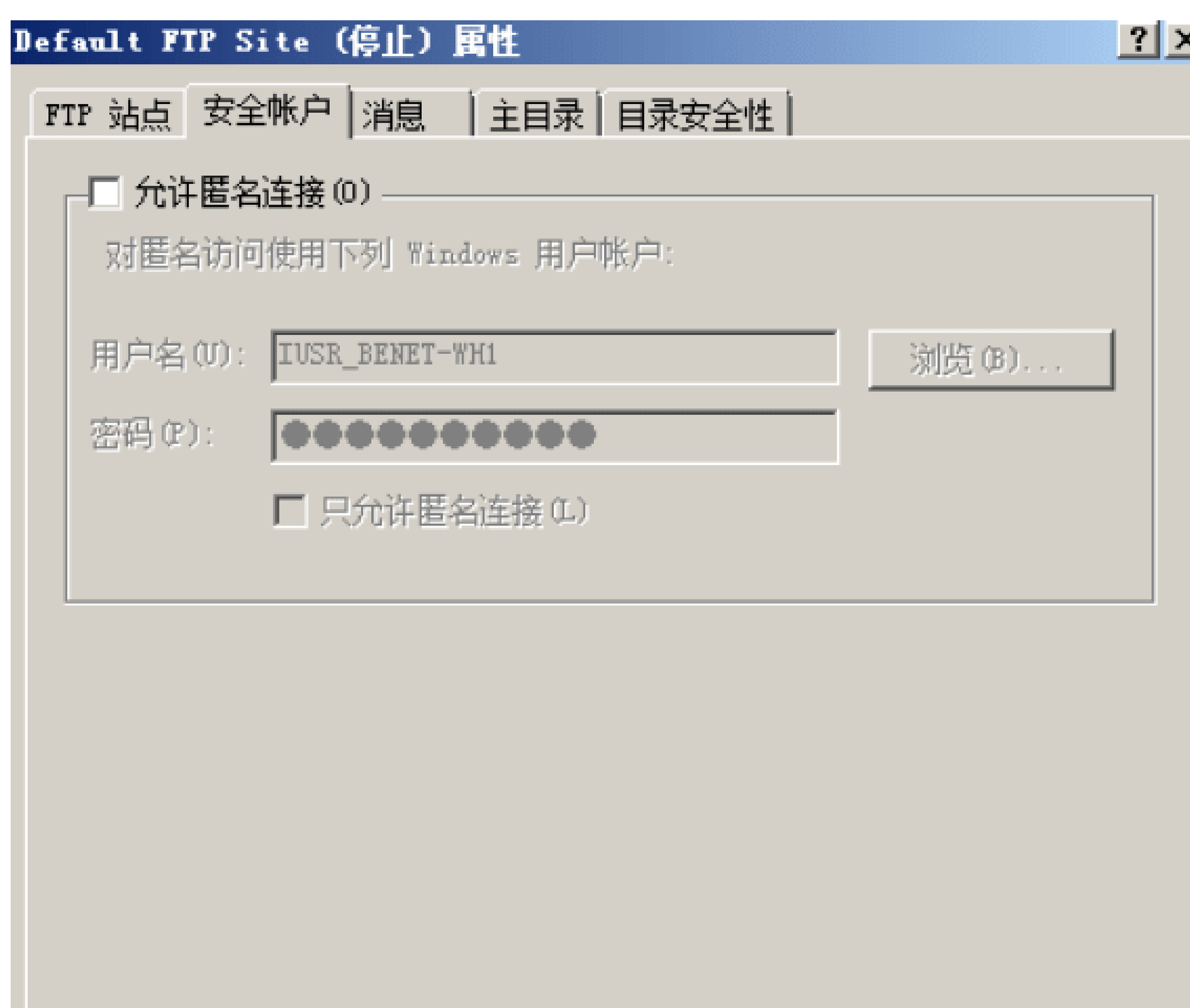


图 4.37　配置 FTP 站点的安全账户

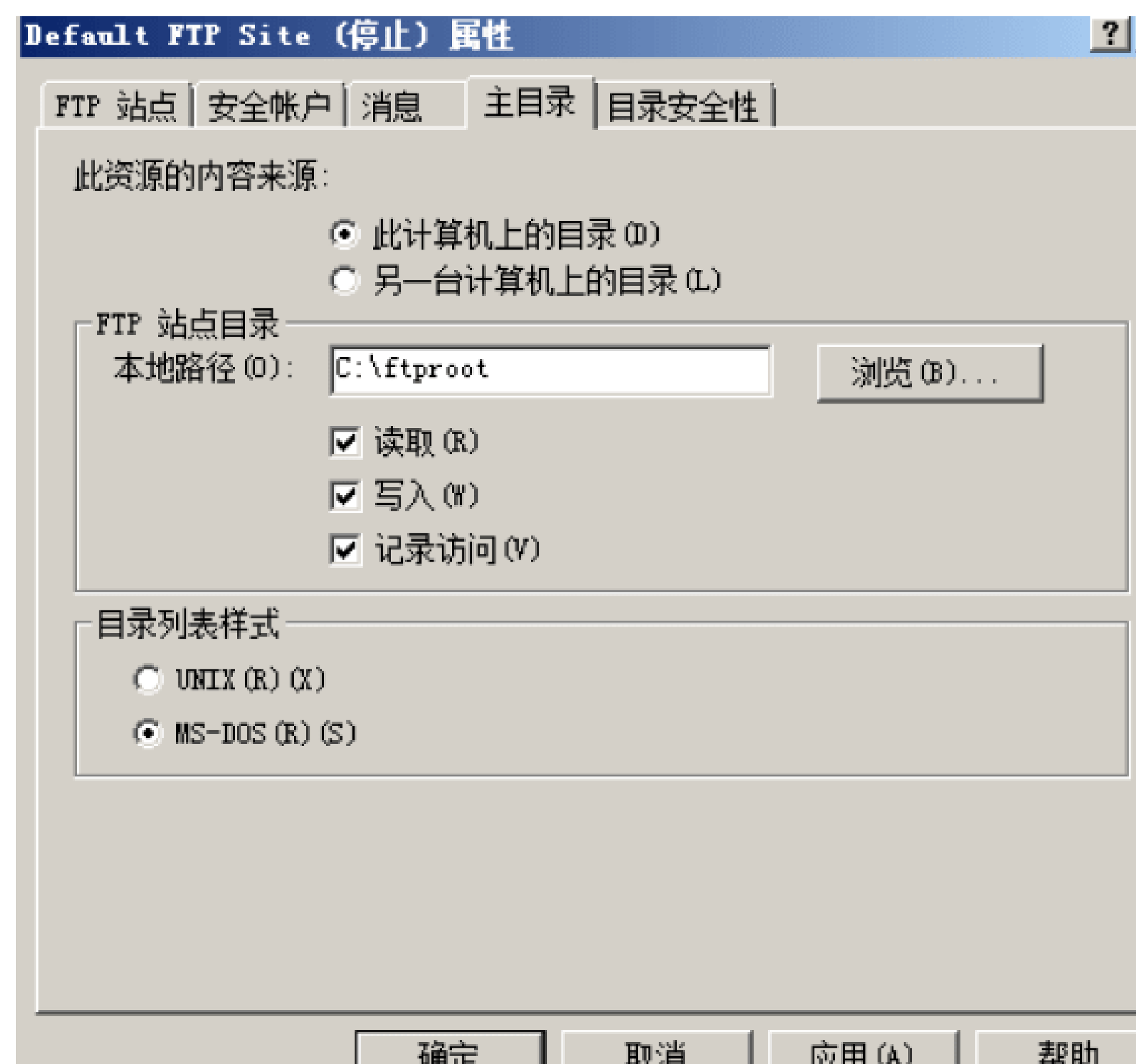


图 4.38　设置主目录路径和访问权限

3. 在客户机上访问 FTP 站点

在客户机上，打开浏览器，输入 ftp://172.16.0.1，访问 FTP 站点，如图 4.39 所示。

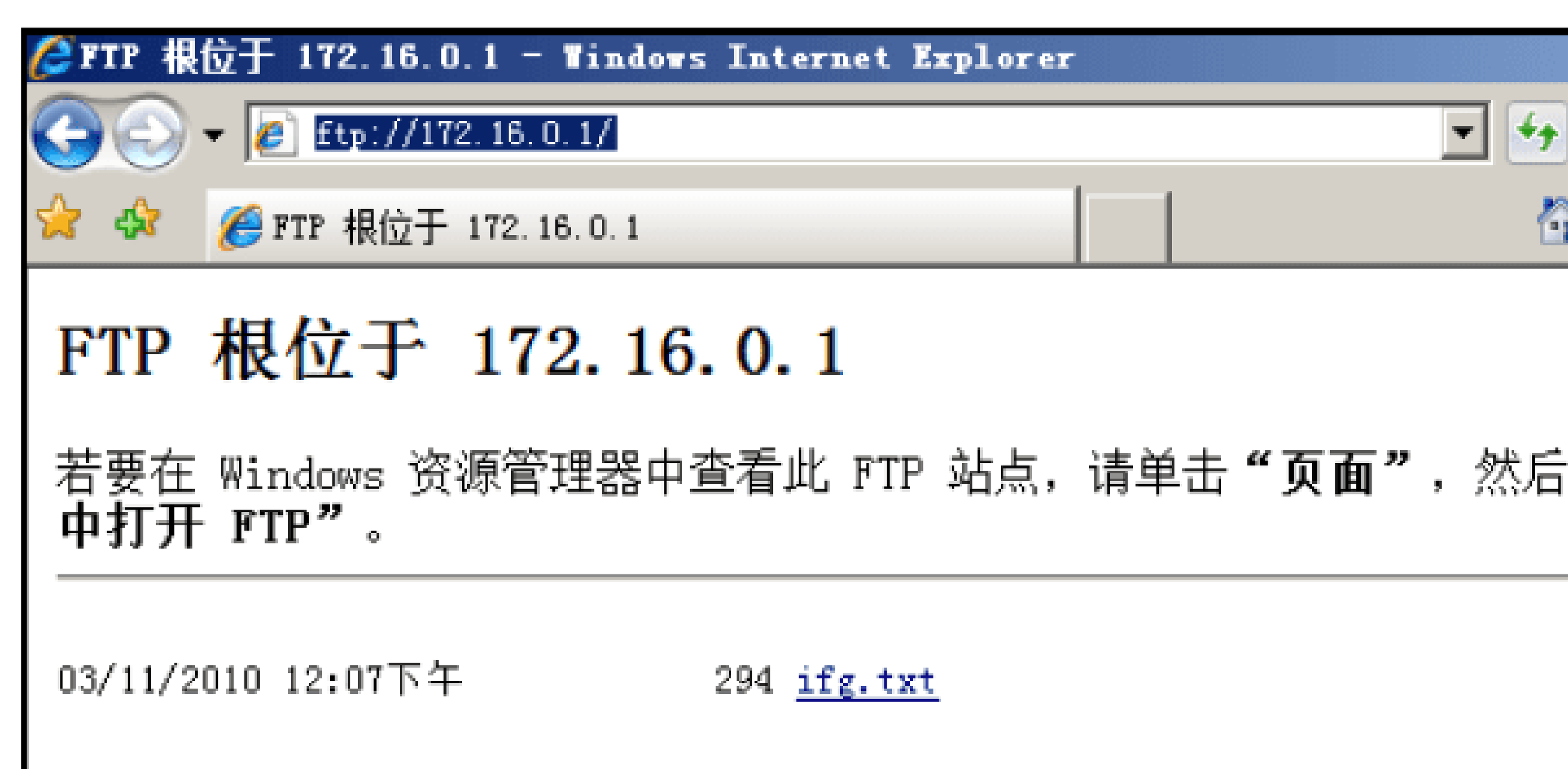


图 4.39　成功访问 FTP 站点

六、附加实验

（1）利用命令提示符和第三方软件访问 FTP 站点。
（2）用 sever-U 创建 FTP 站点。

七、分析与讨论

如何从客户机匿名访问 Web 站点？

实验 13　Web 服务器配置

一、实验说明

World Wide Web 的中文名为万维网（也称为“网络”、WWW、3W 或 Web），它是一个资料空间。在这个空间中，一样有用的事物，称为一样“资源”；并且由一个全域“统一资源标识符”（URL）标识。这些资源通过超文本传输协议（hypertext transfer protocol）传送给使用者，而使用者通过单击链接来获得资源。从另一个观点来看，万维网是一个通过网络存取的互联超文件（interlinked hypertext document）系统。

二、实验目的

（1）掌握在 Windows 上进行 Web 服务器配置的方法。
（2）加深对客户机/服务器模式的理解。
（3）熟悉服务器配置向导的使用方法。

三、实验内容

（1）Web 站点的规划。
（2）管理默认的 Web 站点。
（3）添加新的 Web 站点。
（4）Web 站点的设置和访问。

四、实验准备

安装有 Windows Server 2008 并连接在网络中的计算机。

五、实验参考步骤

1. 添加 Web 服务器角色
① 选择要安装在此服务器上的一个或多个角色，如图 4.40 所示。
② 选择为 Web 服务器（IIS）安装的角色服务，如图 4.41 所示。
③ 成功安装 Web 服务器的角色，如图 4.42 所示。

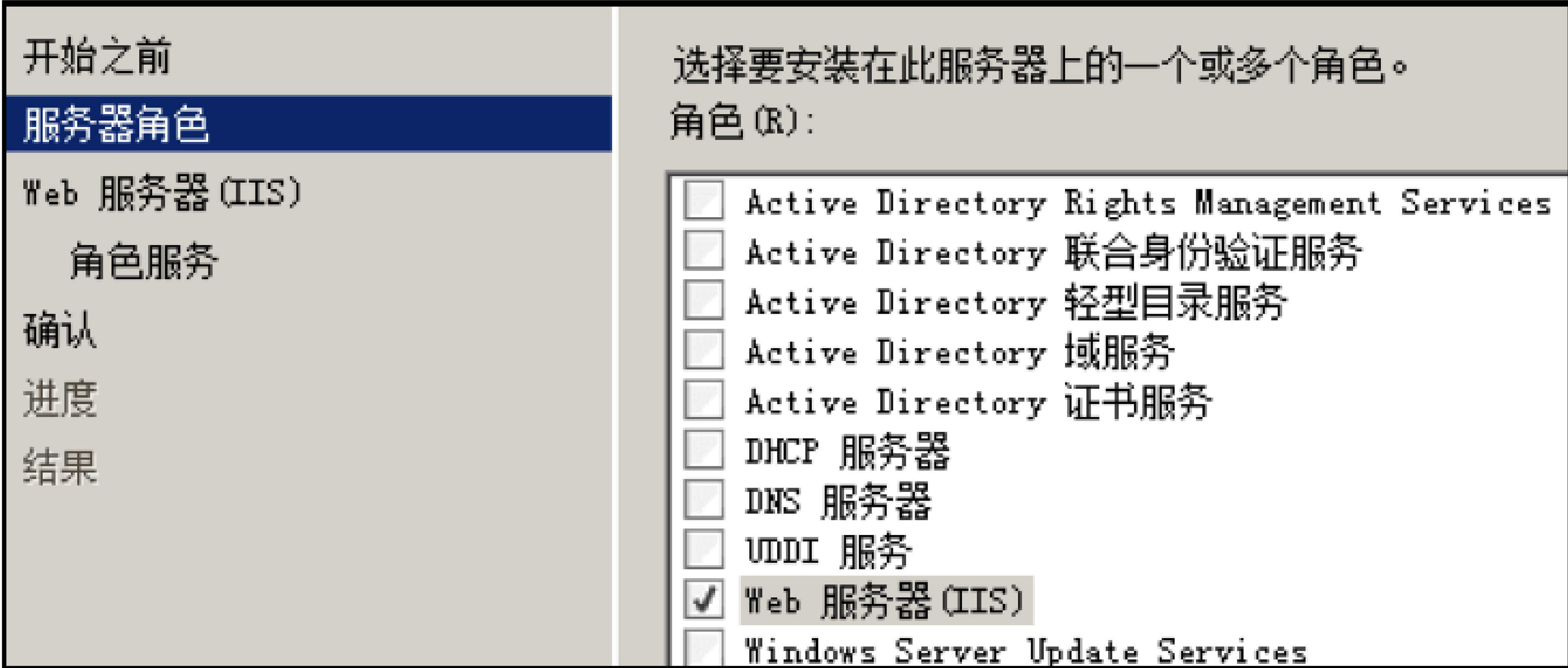


图 4.40　在服务器上安装 Web 服务器角色

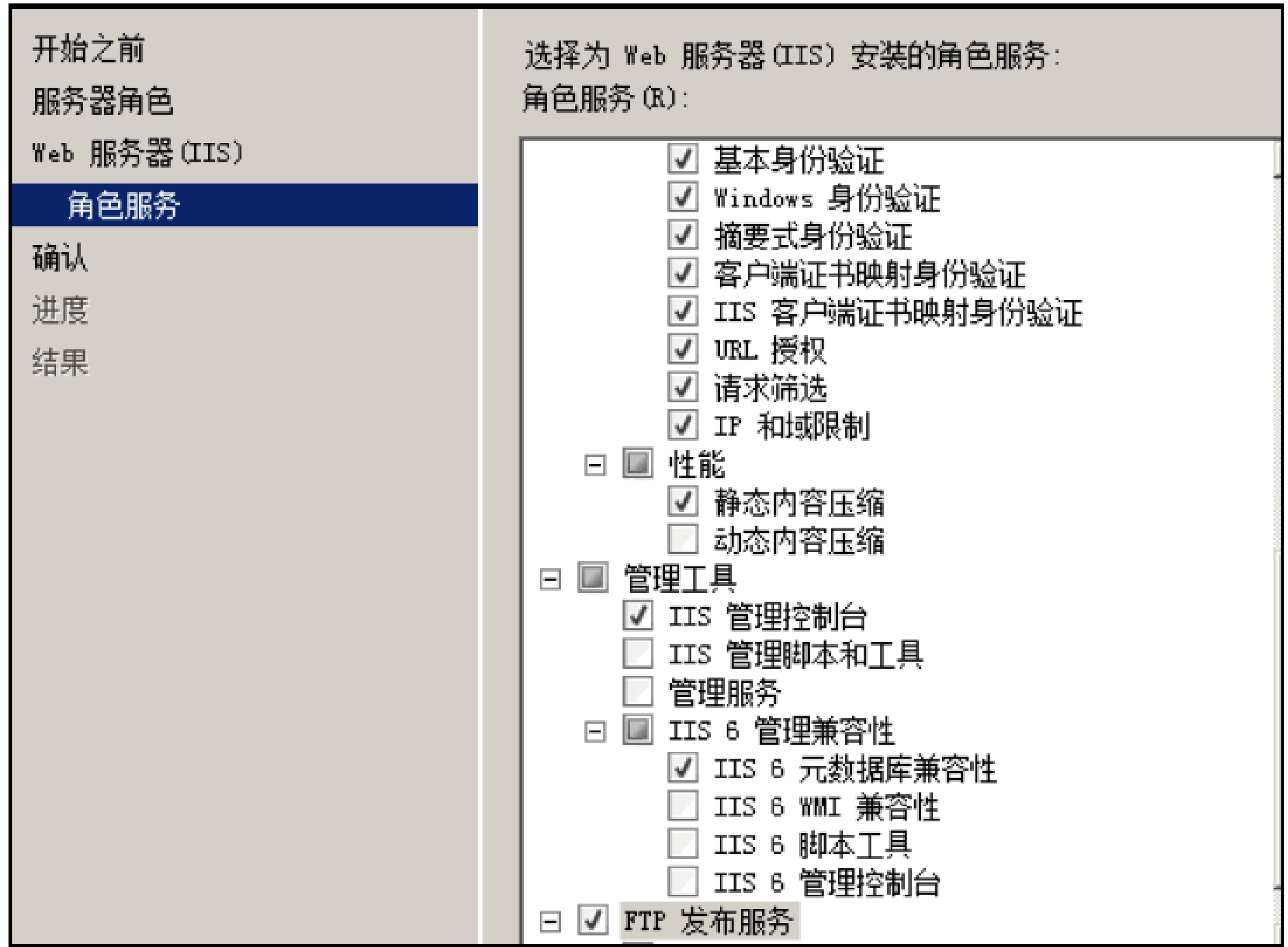


图 4.41　选择为 Web 服务器安装的角色服务

2. 添加主机记录

新建 Web 主机，域名和 IP 地址如图 4.43 所示。

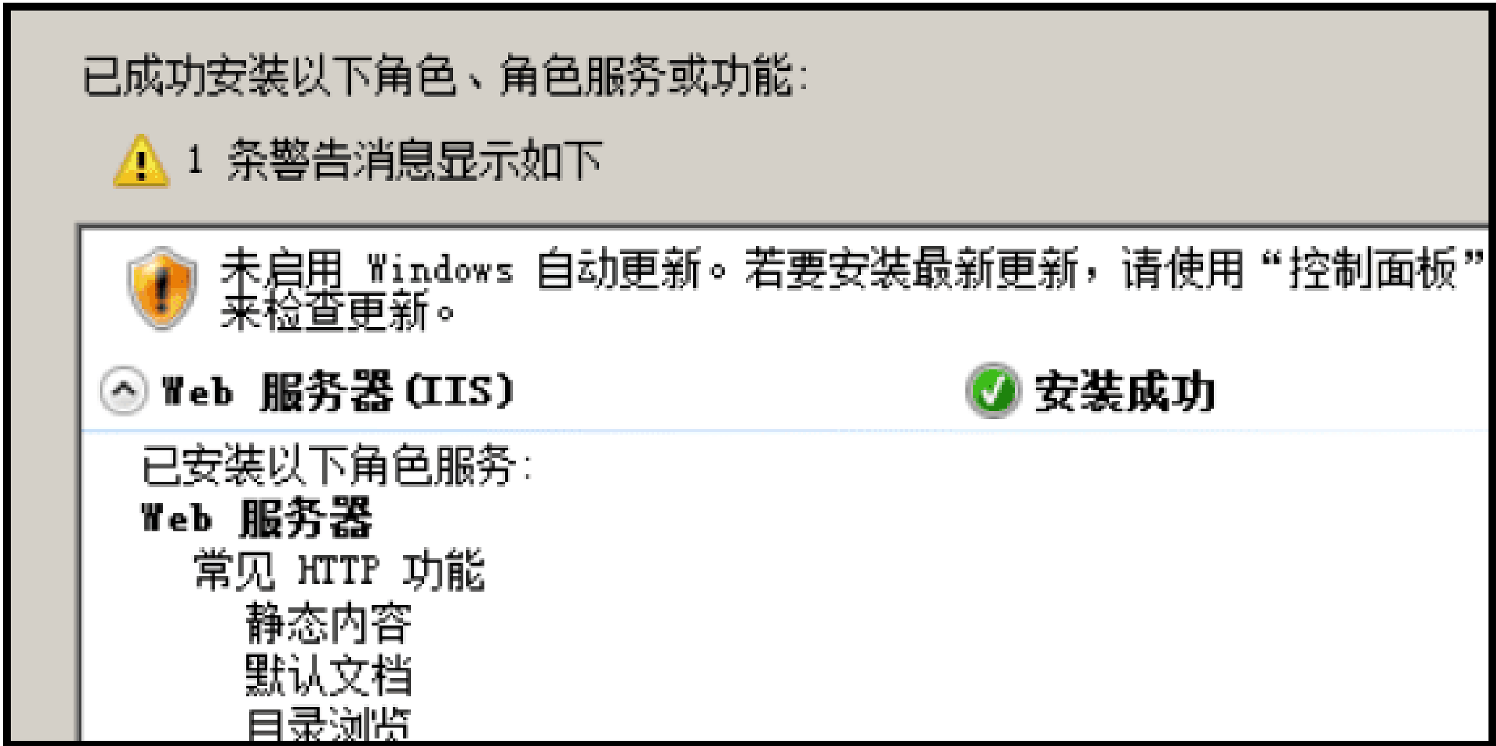


图 4.42　成功安装 Web 服务器的角色



图 4.43　新建 Web 主机

3. 创建新站点

① 选中默认的 Web 服务器，右击，选择“添加网站”命令，弹出如图 4.44 所示的对

话框。

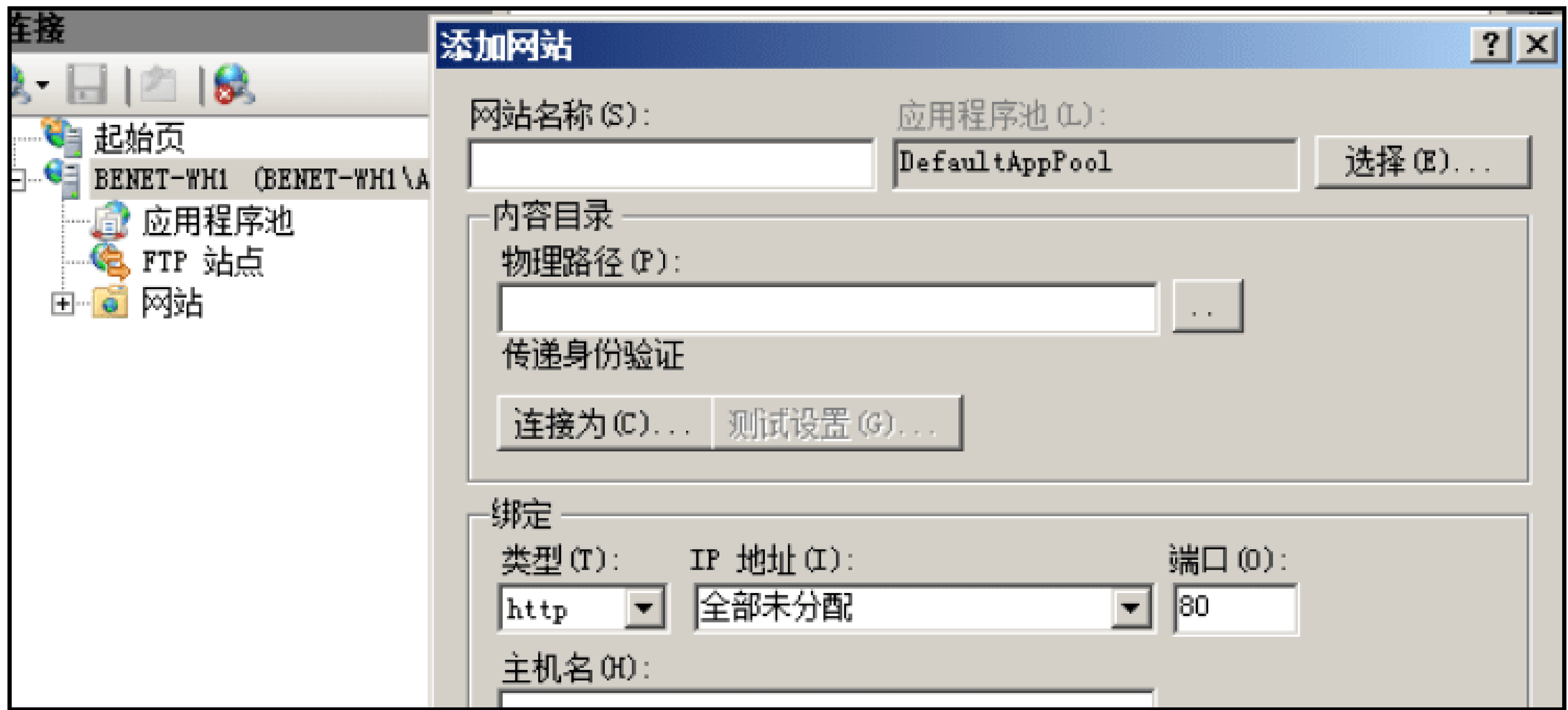


图 4.44　打开“添加网站”对话框

② 输入网站名称为 IFG，并选择网页保存的物理路径，如图 4.45 所示。

4. 禁用匿名身份验证，启用基本身份认证

① 选择新建的 Web 站点 IFG，打开“身份验证”窗口，如图 4.46 所示。

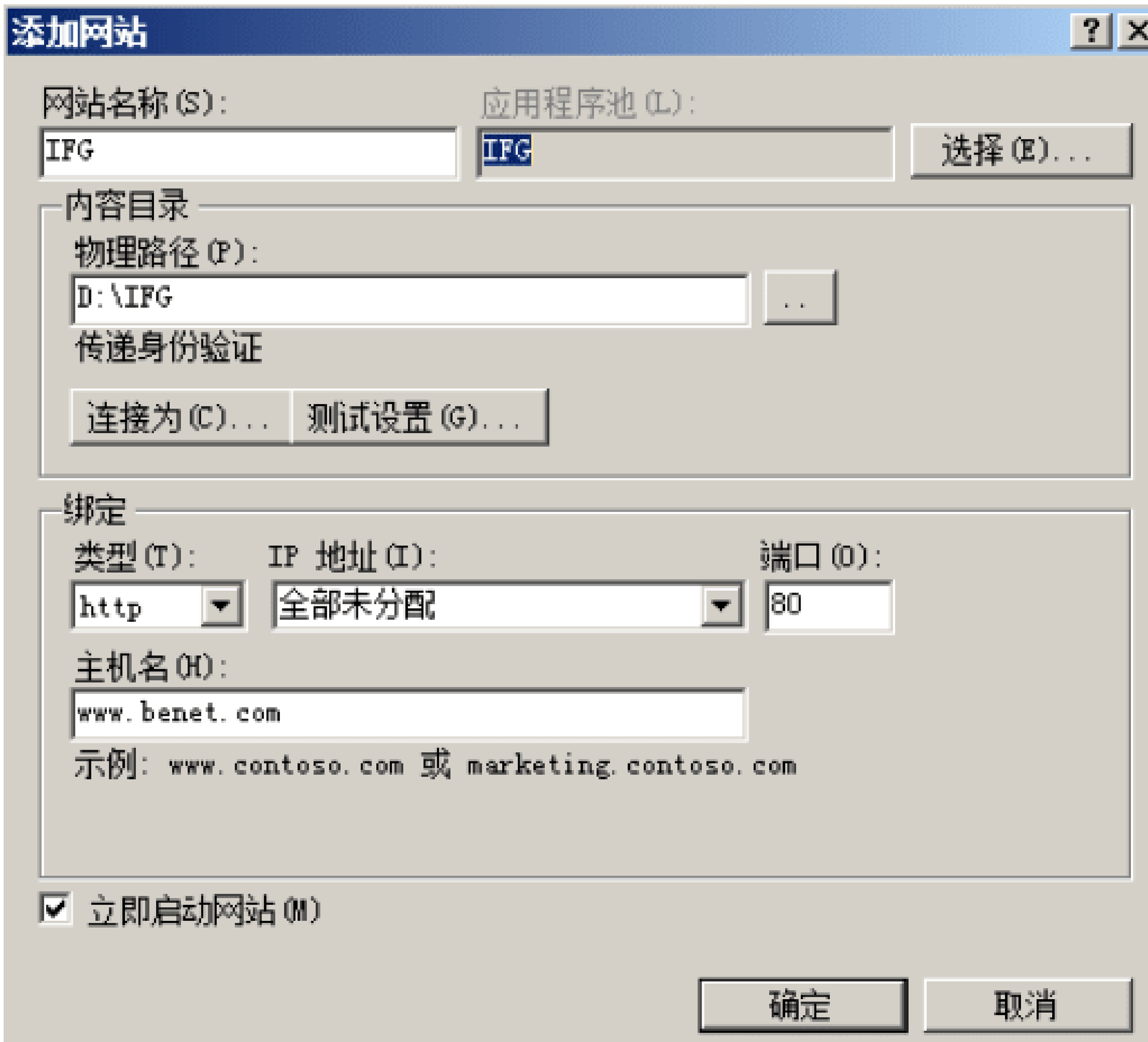


图 4.45　配置网站名称及选择物理路径

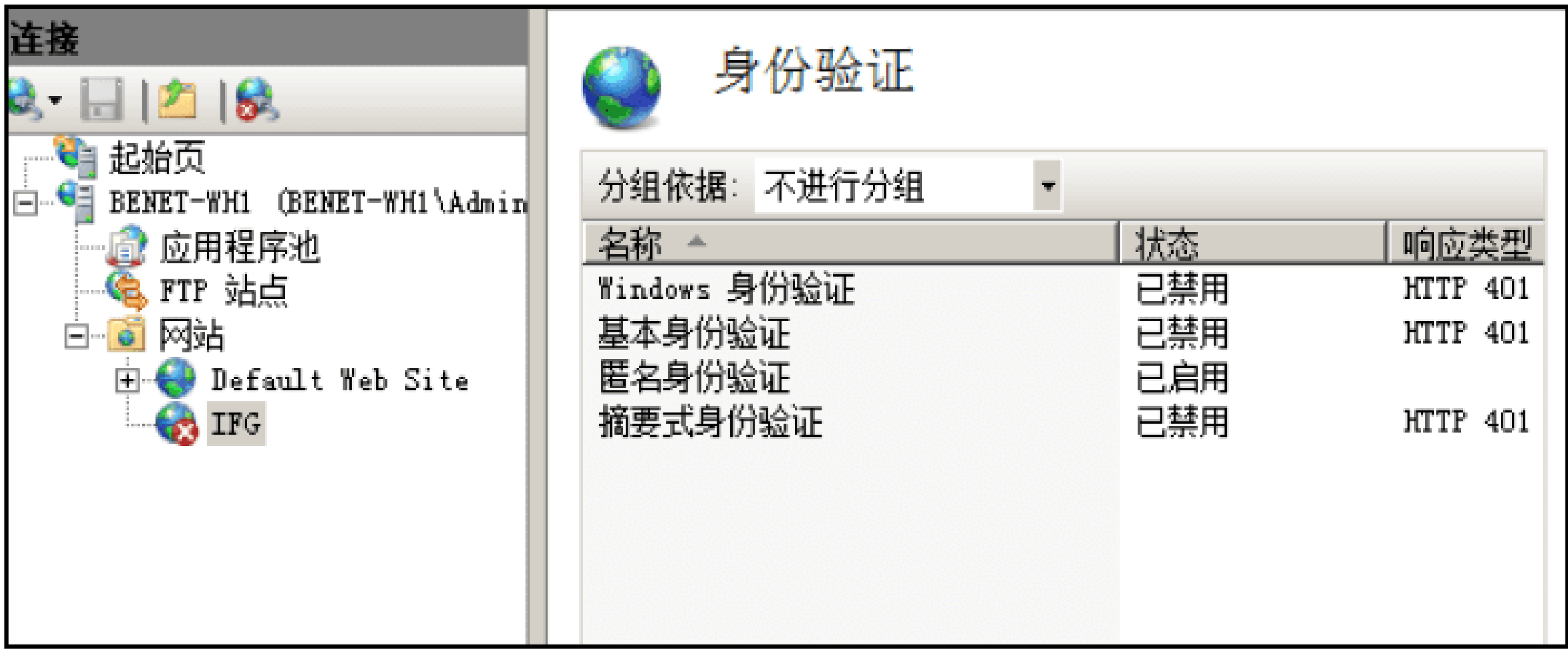


图 4.46　打开“身份验证”窗口

② 选择“匿名身份验证”选项，将其设置为“已禁用”，如图 4.47 所示。

③ 选择“基本身份验证”选项，将其设置为“已启用”，如图 4.48 所示。

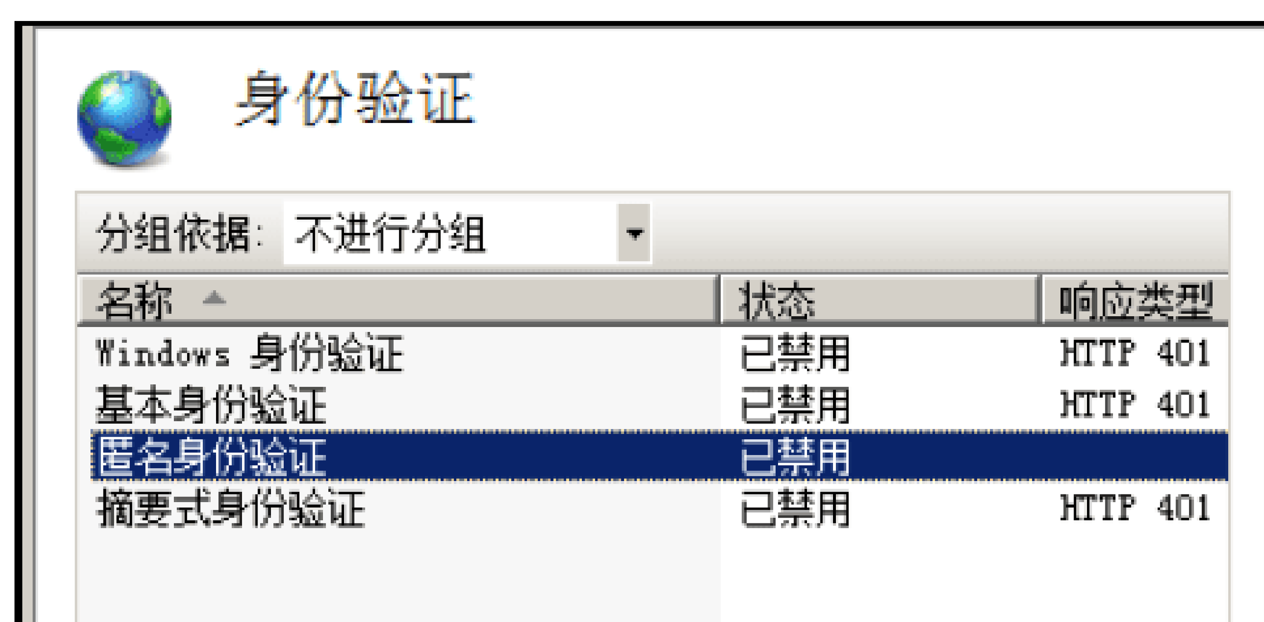


图 4.47　禁用匿名身份验证

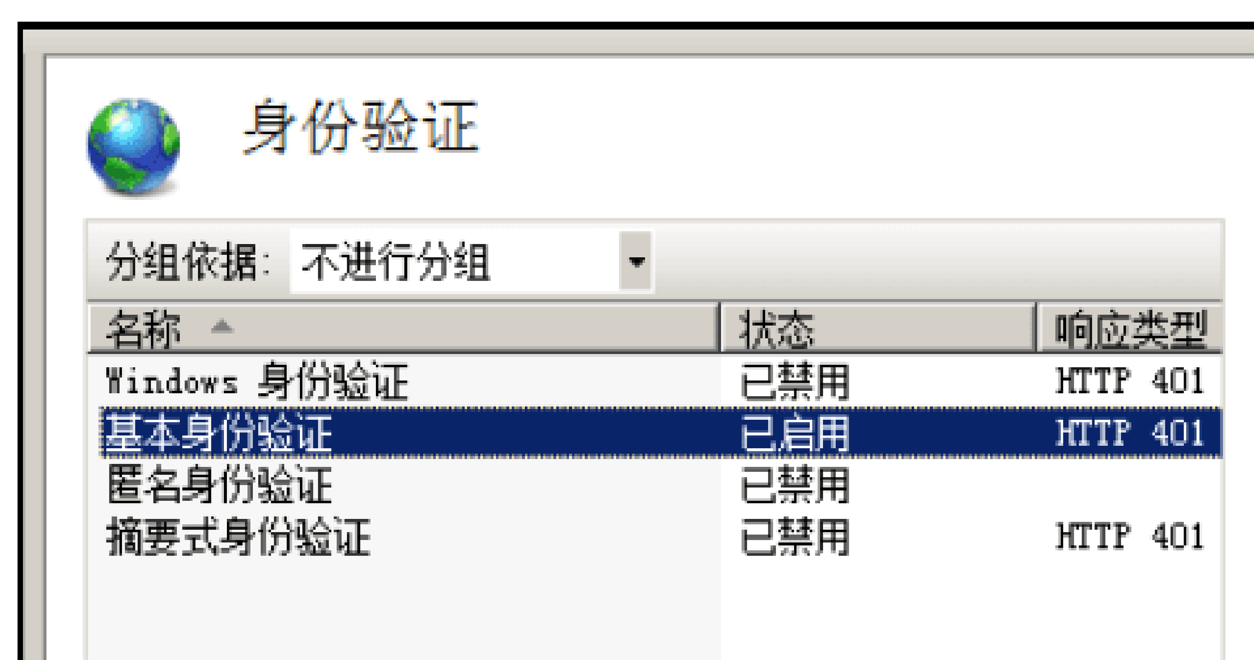


图 4.48　启用基本身份验证

5．*客户使用用户名和密码访问该站点*

在客户机中，输入网址 http://www.benet.net，在弹出对话框中输入预先设定好的用户名和密码访问 Web 站点，如图 4.49 所示。

输入正确的“用户名”和“密码”后，单击“确定”按钮，会显示成功登录到新建的 Web 站点，如图 4.50 所示。



图 4.49　访问 Web 站点

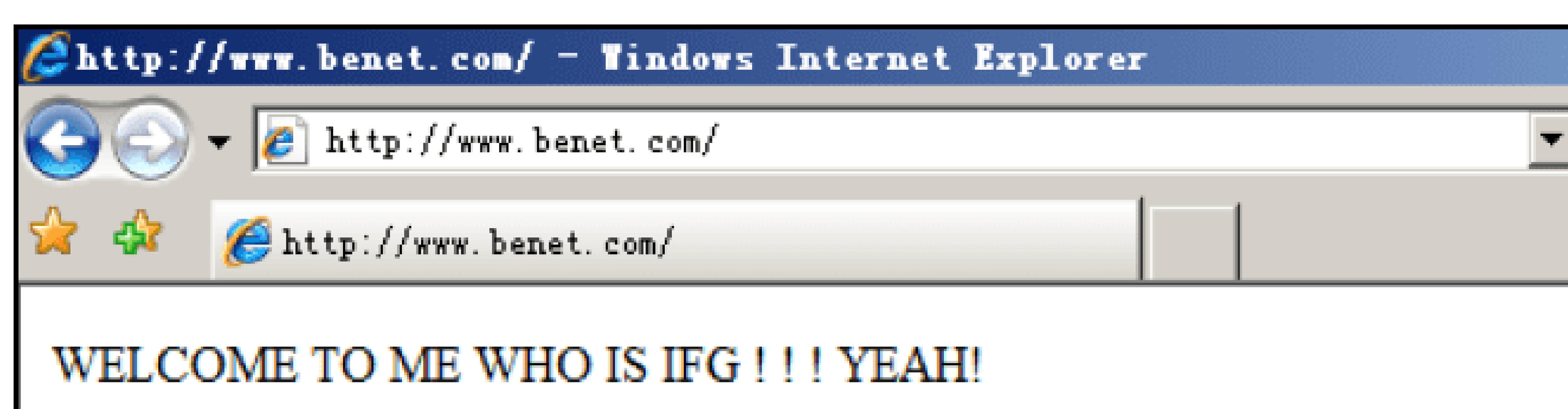


图 4.50　登录 Web 站点

六、附加实验

（1）使用不同的 IP 地址创建 Web 站点。
（2）使用不同的端口号创建不同的 Web 站点。

七、分析与讨论

如何从客户机访问 Web 站点？

习　题　4

一、选择题

1．下列网络应用中，访问的用户越多，速度越快的是【　　】。
　A．网页浏览　　B．电子邮件　　C．FTP　　D．BT下载

2．在下面的协议中，【　　】不是运行在TCP/IP应用层。

A．Telnet　　B．TCP　　C．FTP　　D．DNS

3．我们平时用的QQ属于【　　】。

A．电子公告板　　B．网络日志　　C．网络论坛　　D．即时通信

4．在FTP服务器默认预置的端口中，连接建立后始终保持打开的端口是【　　】。

A．20　　B．21　　C．22　　D．23

5．在Windows组件向导中，“Internet信息服务（IIS）”不包含下列【　　】子组件。

A．WWW服务器　　B．FTP服务器

C．Internet服务管理器　　D．DNS服务器

6．已知接入Internet网的计算机用户为Xinhua，而连接的服务商主机名为public.tpt.tj.cn，则相应的E-mail地址为【　　】。

A．Xinhua@publiC.tpt.tj.cn　　B．@XinhuA.publiC.tpt.tj.cn

C．XinhuA.public@tpt.tj.cn　　D．publiC.tpt.tj.cn@Xinhua

7．电子邮件的特点之一是【　　】。

A．采用存储—转发方式在网络上传递信息，不像电话那样直接、即时，但费用较低

B．在通信双方的计算机都开机工作的情况下方可快速传递数字信息

C．比邮政信函、电报、电话、传真都更快

D．只要在通信双方的计算机之间建立起直接的通信线路后，便可快速传递数字信息

8. 下列【　　】协议属于应用层协议。

A．IP，TCP和 UDP　　B．FTP，SMTP和Telnet

C．ARP，IP和UDP　　D．ICMP，RARP和ARP

二、填空题

1．统一资源定位器的格式为________________。

2．在网络中，一般的Web站点的默认TCP端口号是________。

3．FTP最大的特点是用户可以使用Internet上众多的匿名FTP服务器，登录匿名FTP服务器时使用的用户名是________。

4．下面是打乱次序的DHCP服务的基本流程，请写出它的正确次序________。

A．DHCP客户机发出请求信息　　B．DHCP服务器发出提供信息

C．DHCP客户机发出探测信息　　D．DHCP服务器发出确认信息

5．DHCP服务器配置完成后，请写出在客户端查看TCP/IP配置的命令。

A．________：显示客户端TCP/IP的详细配置信息；

B．________：手工释放IP地址；

C．________：重新获取IP地址。

三、简答题

1．使用的C/S模式的主要优点有哪些？

2．简述B/S工作模式与C/S工作模式有何异同。

3．为什么在FTP中，客户对控制连接发出主动打开命令，而对数据连接要发出被动打开命令？

4．微博有哪些特点？

5．简述HTTP的工作机制。

第 5 章　IEEE 802 组网技术

IEEE 802 成立以后，已经推出了一系列标准。这一系列标准中的每一个子标准都由委员会中的一个专门工作组负责。IEEE 802 委员会前有 20 多个分委员会。图 5.1 为 IEEE 802 体系结构。

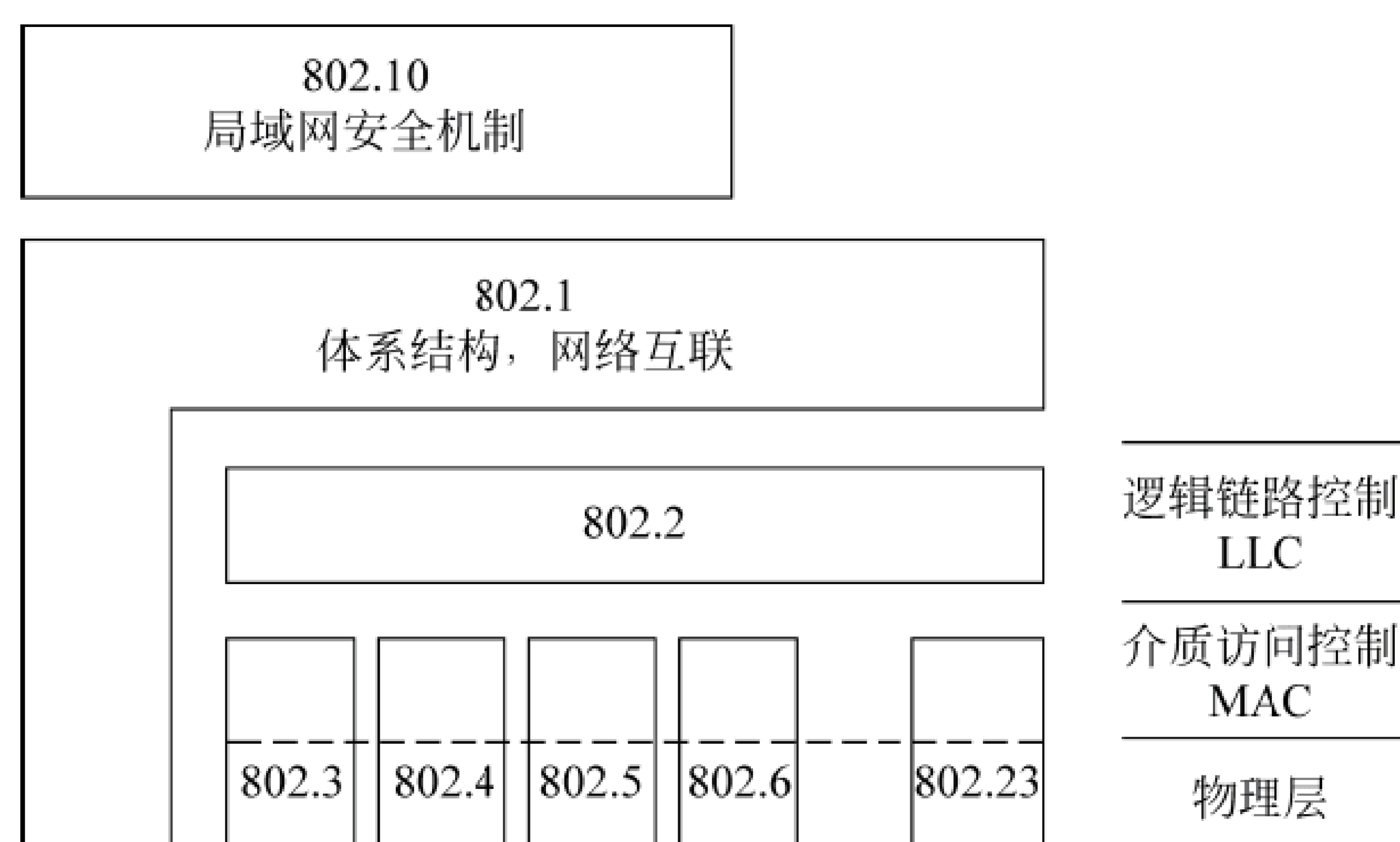


图 5.1　IEEE 802 体系

在 IEEE 802 庞大的标准体系中，目前影响最大、应用最广的是如下 3 个子协议/子系列：

- 面向以太网的 IEEE 802.3 子系列。
- 面向虚拟局域网的 IEEE 802.1q。
- 面向无线局域网的 IEEE 802.11。

5.1　以太网技术

5.1.1　以太网的发展

以太网已经成为当今局域网的一个工业标准。以太网（Ethernet）是一种以早先人们想象的传播电磁波的介质 Ether 命名的计算机网络，于 1975 年由 Xerox 公司推出。当时采用的是同轴电缆连接（最早是粗同轴电缆——10BASE-5，后来改用价格比较便宜的细同轴电缆——10BASE-2），形成一种总线式结构，如图 5.2 所示。

由于同轴电缆连接的网络在安装、扩充和维护都很不方便，不能满足局域网飞速发展的需要，1983 年就开始采用 Hub 连接、非屏蔽双绞线传输的星形结构，被命名为 10BASE-T，如图 5.3 所示。需要注意的是，这种星形结构在逻辑上还是总线型的，因为它还是一种共享工作模式。

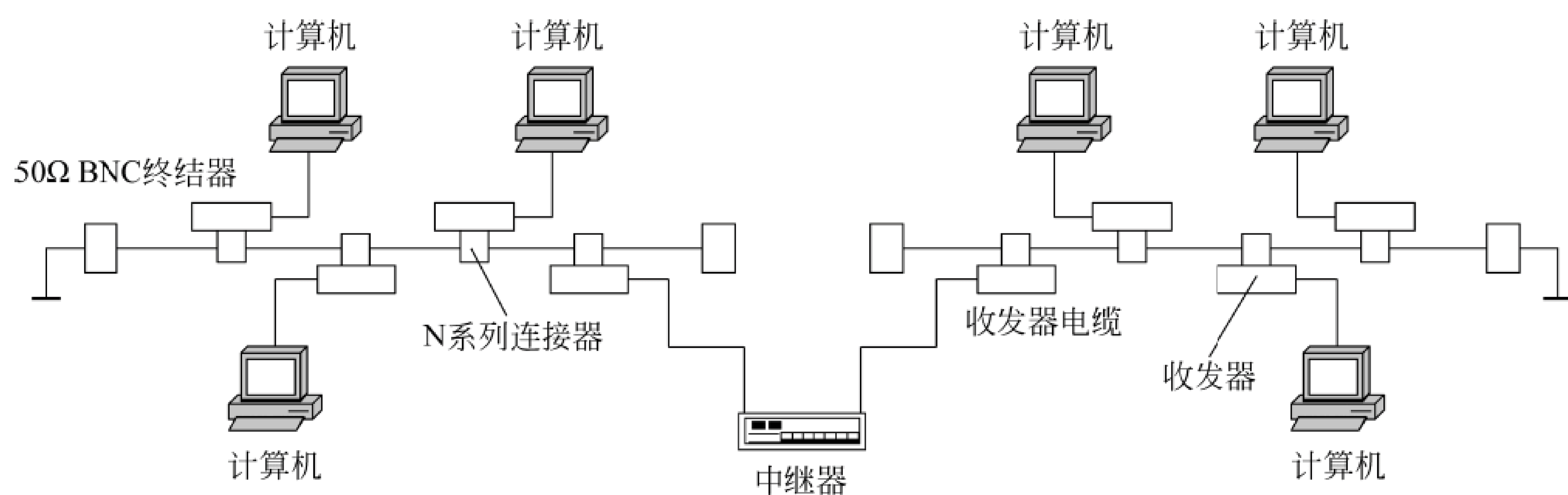


图 5.2　10BASE-5 以太网结构图

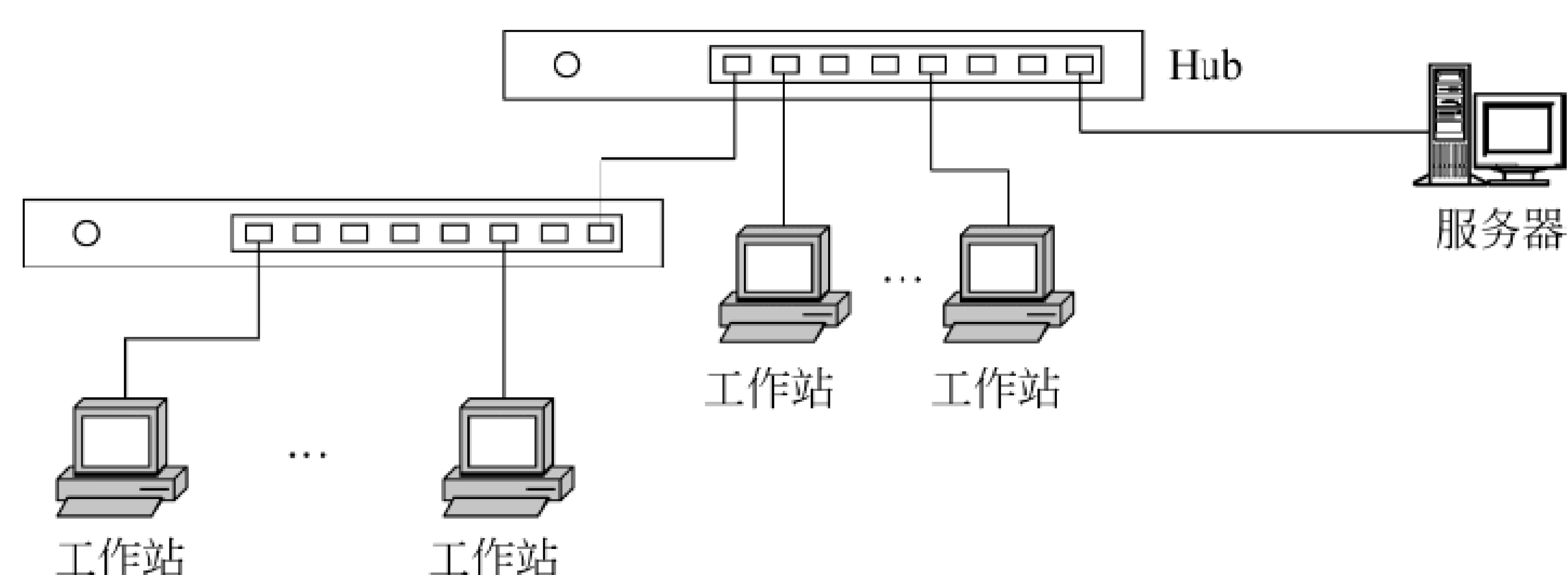


图 5.3　10BASE-T 以太网结构图

10BASE-T 以太网的基本参数如下：

- Hub——集线器，可将接收的数据分发到各端口，每个端口的速率为 10Mbps；
- 双绞线——两端用 RJ-45 分别与 Hub 和计算机连接。

10BASE-T 以太网的主要性能指标：

- 集线器与网卡、集线器之间的最长距离为 100m；
- 最长两点之间的距离不超过 500m；
- 不使用网桥时，最多接入站点数为 1023。

以后，以太网不断发展，但很长时间内基本上都保持了这种基本的结构形式。表 5.1 为采用集线器的以太网发展情况。

表 5.1　采用集线器连接的以太网发展情况

类型	IEEE 802 标准	标准批准时间	带宽（bps）	通信交互方式	以太网名称	传输介质	网段最大长度（m）
标　准以太网	802.3	1983	10M	半双工	10BASE-T	UTP	100
快　速以太网	802.3u	1995	100M	全双工	100BASE-TX	两对 UTP5 类线/STP	100
					100BASE-FX	两根光纤（发送、接收各一根）	2k
				半双工	100BASE-T4	4 对 UTP3 类/5 类	100

续表

类型	IEEE 802 标准	标准批准时间	带宽（bps）	通信交互方式	以太网名称	传输介质	网段最大长度（m）
千兆位以太网	802.3z	1997	1G	全半双工	1000BASE-SX	850nm 激光器多模光纤（62.5/50μm）	550
					1000BASE-LX	1300nm 激光器多模光纤（62.5/50μm）	550
						1300nm 激光器 10μm 单模光纤	5k
					1000BASE-CX	两对短距离屏蔽双绞线	25
	802.3ab	1997	1G	全/半双工	1000BASE-T	4 对 UTP5 类线	100
万兆位以太网	802.3ae	2002.6	10G	全/半双工	10GBASE-SR	850nm 激光器的多模光纤	300
					10GBASE-LR	1300nm 激光器的单模光纤	10k
					10GBASE-ER	1500nm 激光器的单模光纤	40k
	802.3ak	2004	10G	全/半双工	10GBASE-CX4	4 对双芯同轴电缆	15
	802.3an	2006	10G	全/半双工	10GBASE-T	4 对 UTP6A 类	100
40G/100G 以太网	802.3ba	2010.6	40G/100G	全双工	40G/BASE-KR4	背板	1
					40G/100GBASE-CR4/10	铜缆	7
					40G/100GBASE-SR4/10	多模光纤	100
					40G/100GBASE-LR4/10	单模光纤	10k
					100GBASE-ER10	单模光纤	40k

说明：

（1）4 对线并非 4 条 2 芯电缆，可以是 4 对双绞线电缆，就是一根网线。同轴电缆也有类似概念。对于光纤则可以采用 4 个波长复用。

（2）从表 5.1 中可以看出，随着传输技术的发展，以太网的最小网段长度已经突破了一般局域网概念中的覆盖范围。这也说明，现在局域网与城域网的界线正在模糊，因此人们常用园区网来称呼它们。

（3）半双工采用集线器连接，形成共享介质并共享带宽模式。全双工采用交换机连接，形成分配带宽模式。图 5.4 为两种传输网络的结构比较。关于冲突域的概念，将在 5.1.2 节介绍。

5.1.2　共享以太网中的 CSMA/CD 协议

1. 多路访问与冲突

介质访问控制（Medium Access Control，MAC）协议也称多路访问控制协议，是用于在共享信道上有效、合理地分配信道资源的控制机制。它是局域网网卡功能的重要组成部分。

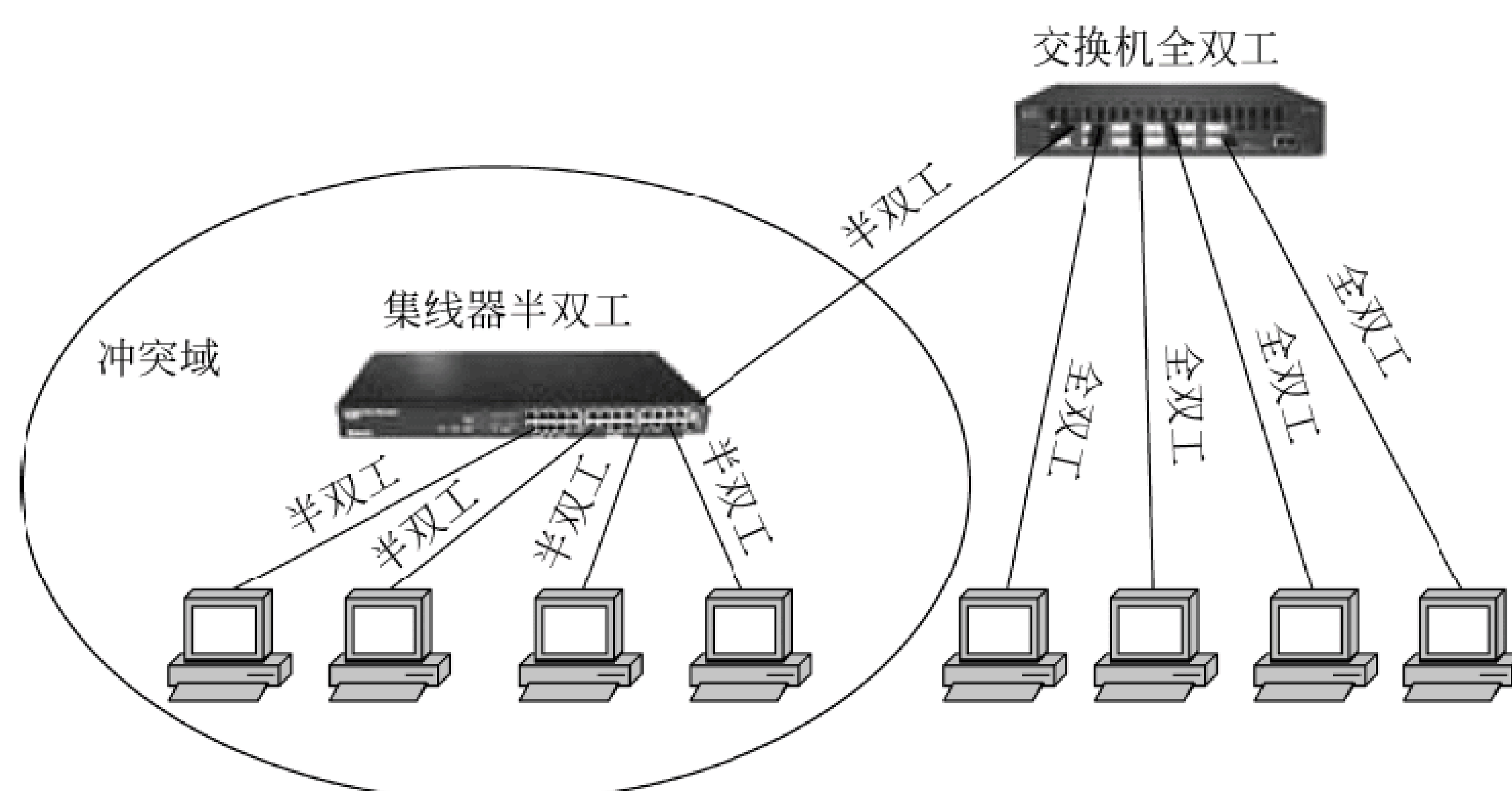


图 5.4　全双工以太网与半双工以太网结构

多路访问与多路复用不同。多路复用是将一条信道静态地分割成多条逻辑信道，使多个用户信息在同一信道上同时传输的技术。但是用静态分配的方法不能有效地处理多路访问问题，因为每路用户的数据发送都具有突发性。突发性可能引起多个用户争相使用介质造成信道冲突（Collision，也称碰撞），使发生冲突时的发送都遭到失败。面对竞争，介质访问控制协议有两种处理方式。

（1）避免冲突。即避免竞争出现，具体地说，就是采用控制授权，形成一种发送受控的方式。例如，使用令牌，只授权给获得令牌的站点才能发送数据。

（2）允许竞争。正视冲突，形成可以随机发送的方式，但是要采取措施尽量减少冲突，降低冲突的影响。例如，带有冲突检测的载波监听多点接入（Carrier Sense Multiple Access With Collision Detection，CSMA/CD）协议就是一种允许冲突的介质的随机发送的多路访问控制协议。

2. CSMA/CD 原理

CSMA/CD 的工作原理有点像多人开讨论会。当一个人想发言时，要先听听有没有人在发言：若有人在发言，就继续听，等等再说；若无人发言，就发言。但是，也许别人也在这么做，出现同时发言的情形，这称为冲突。一旦发生冲突，就立刻停止发言，等一段时间再发言；如果冲突了多次，就暂时放弃发言。上述过程可以简要地叙述为：讲前先听，忙则等待，无声则讲，边讲边听，冲突即停，后退重传。与此相仿，CSMA/CD 具有以下 4 个要点。

（1）MA（Multiple Access，多路访问）——相当于多人讨论。

（2）CS（Carrier Sense，载波侦听）。每个站点在发送数据前，都要先检测信道上有没有脉冲信号，即有没有别的站点在发送数据；没有检测到脉冲信号再发送，否则避让一段时间再继续监听——相当于“讲前先听，忙则等待，无声则讲，边讲边听”。

（3）CD（Collision Detection，冲突检测）。在发送数据的过程中，还要继续监听，目的是发现冲突。一旦发现冲突，立即停止发送，并发出一串阻塞信号，使其他站点也立即停止发送，以便尽快恢复信道，然后避让一段时间再开始监听信道——相当于“冲突即停，后退重传”。

（4）如果 CS 和 CD 过程进行了多次，都没有发送成功，就需要暂时放弃发送——相当于“多次无效，暂缓发送”。

如图 5.5 所示为 CSMA/CD 的基本工作流程。图中，n_r 是已经检测到的碰撞次数，每检测到一次碰撞，n_r 增 1；n_{max} 是设定的最大碰撞次数。

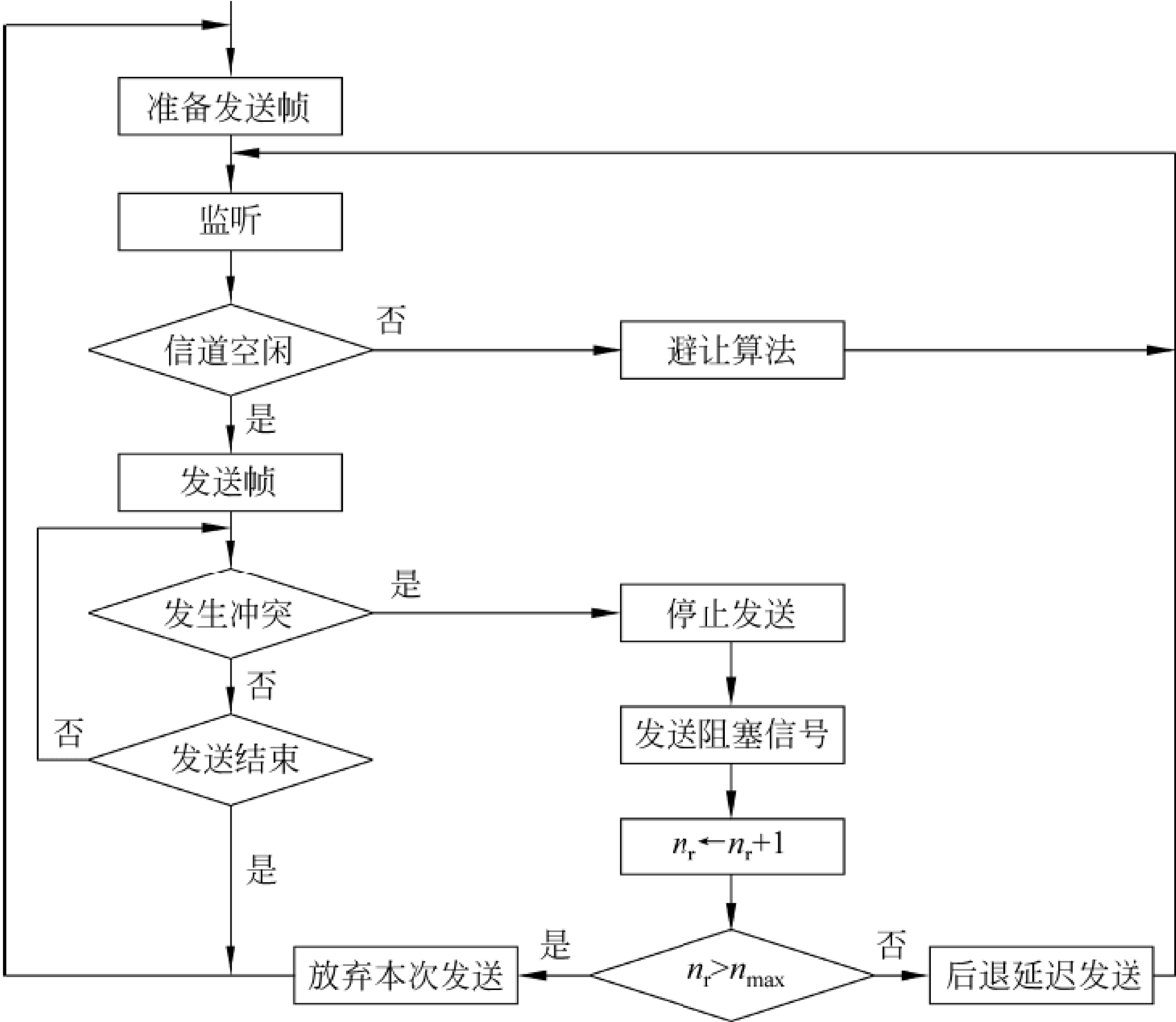


图 5.5　CSMA/CD 的基本工作流程

5.1.3　IEEE 802.3 以太网帧格式

在以太网的发展过程中，先后形成了 5 种帧格式标准：

（1）Ethernet V1（1980）。

（2）Ethernet V2（ARPA，1982）。

（3）RAW 802.3（Novell，1983）。

（4）IEEE 802.3/802.2 LLC（1985）。

（5）IEEE 802.3/802.2 SNAP（1985）。

今天，大多数 TCP/IP 应用都是用 Ethernet V2 帧格式，IEEE 802.3—1997 改回了对这一格式的兼容。这就是现在称为 IEEE 802.3 以太网帧格式。其结构如表 5.2 所示。

表 5.2　IEEE 802.3 以太帧格式

位置	字　段	字段长度（B）	用　　途
帧头	前导码（preamble）	7	同步
	帧开始符（SFD）	1	标明下一个字节为目的 MAC 字段
	目的 MAC 地址	2～6	指明帧的接受者
	源 MAC 地址	2～6	指明帧的发送者
	长度（length）	2	帧的数据字段的长度（长度或类型）
	类型（type）	2	帧中数据的协议类型（长度或类型）

续表

位置	字　段	字段长度（B）	用　　途
数据	数据和填充（data and pad）	46~1500	高层的数据，通常为 3 层协议数据单元。对于 TCP/IP 是 IP 数据包
帧尾	帧校验序列（FCS）	4	对接收网卡提供判断是否传输错误的信息：如果发现错误，则丢弃此帧

注：（1）原则上 MAC 地址可以用 2～6B 来表示，但实际都是 6B。

（2）如果帧长小于 64B，则要求“填充”，以使这个帧的长度达到 64B。

5.1.4　以太网体系结构

图 5.6 为两种典型的以太网体系结构。图 1.56 关于 IEEE 802 体系的具体化。

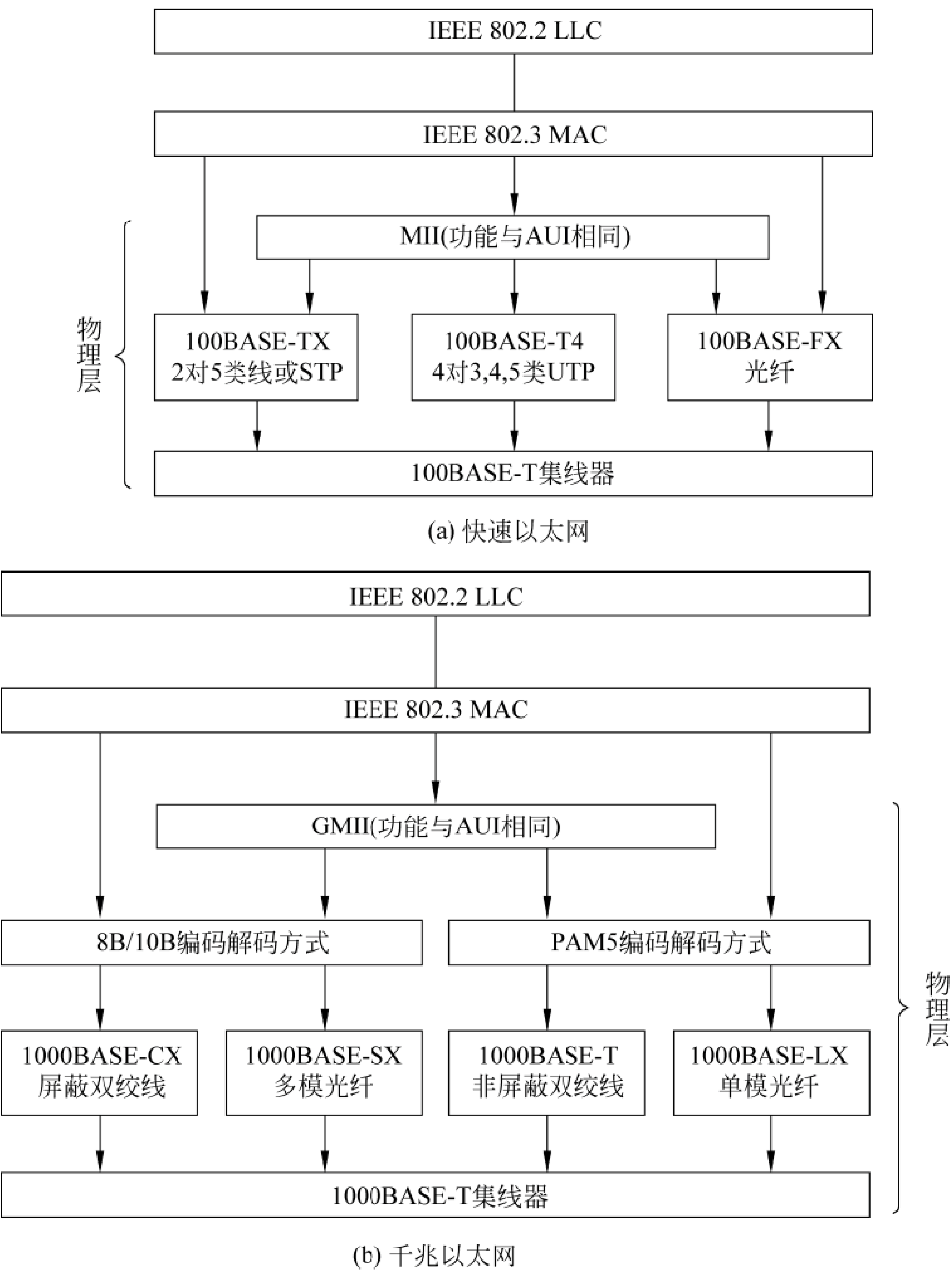


图 5.6　两种典型的以太网体系结构

下面做一些说明：

（1）最下层是集线器，表明这是共享网络，采用半双工工作方式。若把集线器换为交换机，就称为全双工方式。表 5.3 为共享式以太网与交换式以太网的比较。

（2）从下起的第 2 层是传输介质。

表 5.3　共享式以太网与交换式以太网的不同比较

	连接设备	连接设备的工作层次	拓扑结构	通信方式	结点的带宽使用方式
共享以太网	集线器	物理层	逻辑总线结构	广播	共享
交换以太网	交换机	数据链路层	逻辑星形结构	可以点对点	分配

（3）MII（Media Independent Interface，介质独立接口）一般应用于 MAC 层和 PHY 层之间的以太网数据传输，也可叫数据接口。它的一头是二层芯片，另一头是一层芯片。也就是一头是数据源或者说是控制器，另一头是与介质相关的收发器（tranceiver）。千兆以太网中使用的是 GMII。

（4）8b/10b 编码是将一组连续的 8 位数据分解成两组数据：一组 3 位，一组 5 位，经过编码后分别成为一组 4 位的代码和一组 6 位的代码，从而组成一组 10 位的数据发送出去。8b/10b 编码的特性之一是保证 DC 平衡，采用 8b/10b 编码方式，可使得发送的 0、1 数量保持基本一致，并且可以在早期发现数据位的传输错误，抑制错误继续发生。

8b/10b 编码是目前许多高速串行总线采用的编码机制，如 USB3.0、1394b、Serial ATA、PCI Express、Infini-band、Fibre Channel（光纤通道）、RapidIO 等总线或网络等。

用于 1000BASE-T 的符号编码方法。是将从 8B1Q4 数据编码接收到的 4 维五进制符号（4D）用 5 个电压级别（PAM5）传送出去。每个符号周期内并行传送 4 个符号。

5.1.5　基于交换的园区网三层架构

交换式以太网，尤其是单模光纤传输的交换式以太网，可以将传输距离扩大到城域网和广域网的范围，非常适合组建大型网络。这种大型的以太网，常称为园区网。如图 5.7 所示，典型的园区网一般由 3 层组成：核心层、汇聚层和接入层，目的是进行设备的合理配置，以达到良好的经济技术效果。

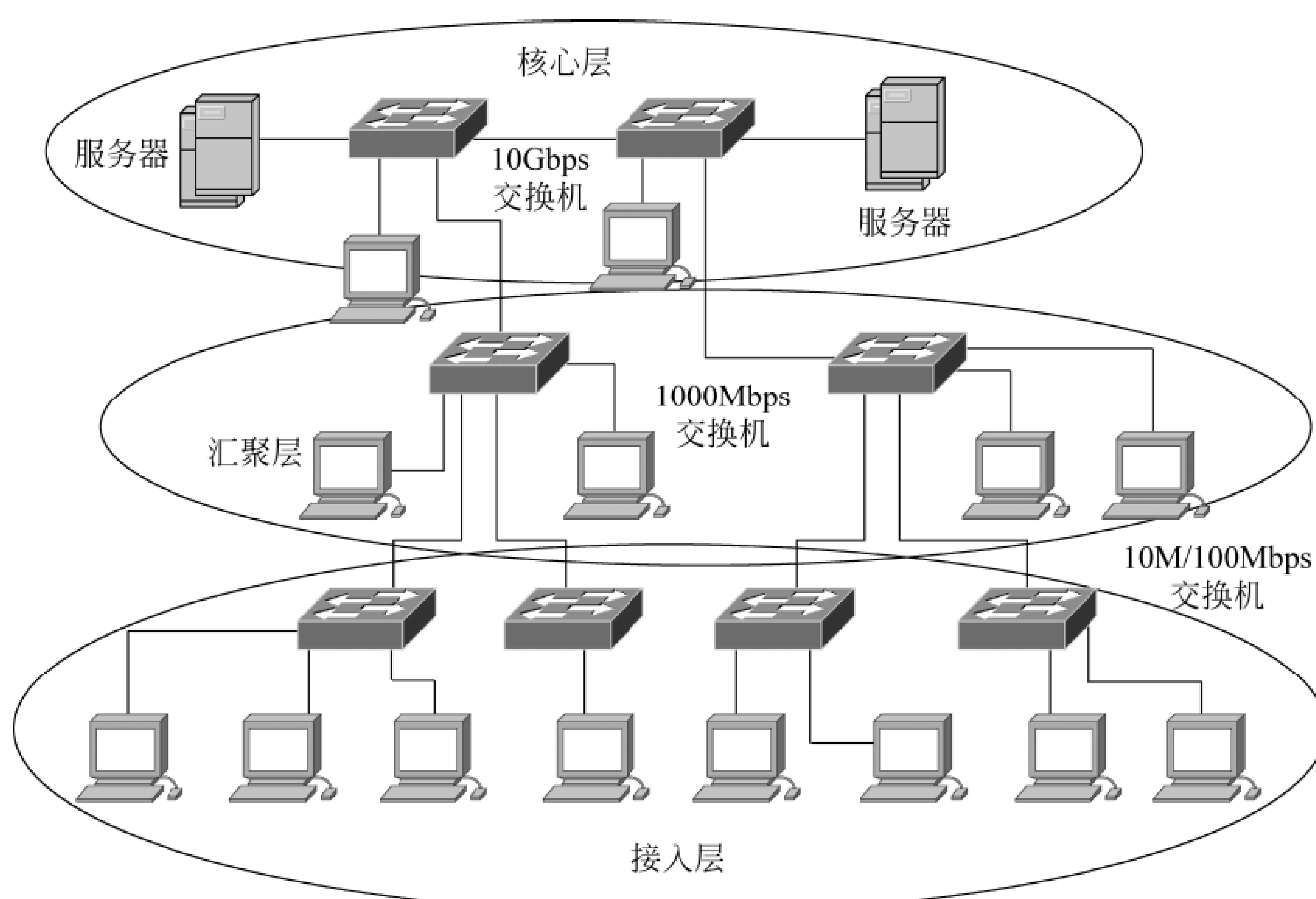


图 5.7　三层网络架构

1．接入层

接入层直接面向工作组或主机，由提供用户物理接入的接入点设备组成，主要作用是为用户接入网络提供支持。由于每一组的主机数量都比较少，流量需求比较低，并且需要为网络提供充分的接入端口，因此接入层所使用的交换机有低成本和高端口密度的特点，并配有高速上联的端口以便接入汇聚层。

2．汇聚层

汇聚层通常作为连接本地小型网络的逻辑中心，是网络接入层各工作组的流量和业务的汇聚点，为它们提供聚合与转发的功能，以减轻核心层设备的负荷。它一方面要能够处理来自接入层设备的所有通信量，另一方面要提供到核心层的上行链路。与接入层交换机相比，汇聚层交换机需要较高的性能、较少的接口和更高的交换速率。

3．核心层

核心层也称骨干层，是网络的枢纽。它对汇聚层的流量和业务进一步汇聚，通过高速转发数据，提供优化、可靠的骨干传输结构。由于流量较大，重要性突出，对整个网络的连通起到至关重要的作用，在可靠性、高效性、冗余性、容错性、可管理性、适应性、低延时性等方面也具有更高的要求，通常选择高带宽（千兆以上）的设备。为了提高可靠性，也使负载均衡、网络性能改善，还常常选择双机冗余热备份。

说到底，这样的结构就是汇聚再汇聚-交换再交换结构。因此，并不局限于三层，也可以做成四层、五层，或简化为二层。

5.2　虚拟局域网

5.2.1　虚拟局域网概述

虚拟局域网（Virtual LAN，VLAN）就是按照某种要求由一些局域网段构成的与物理位置无关的逻辑组。划分在这个逻辑组中的网段或站点，可以来自一个物理的局域网，也可能来自互相连接的不同的局域网中；还可以将一个物理的局域网中的站点，划分在不同的逻辑组中，形成不同的 VLAN。

在传统的局域网中，任何一个站点所发送的广播数据包都将转发至网络中的所有站点。而在交换式以太网中，VLAN 技术使得网络的拓扑结构变得非常灵活，如位于不同楼层的用户或者不同部门的用户根据需要加入不同的 VLAN。这些用户可以处在不同的物理 LAN 上，但它们之间可以像在同一个 LAN 上那样自由通信而不受物理位置的限制。网络的定义和划分与物理位置和物理连接没有任何必然的联系。网络管理员可以根据不同的需要，通过相应的网络软件灵活地建立和配置虚拟网，并为每个虚拟网分配它所需要的带宽。

在大型局域网中，VLAN 技术给网络管理员和网络用户都带来了许多好处，归纳起来主要有以下几点：

- 简化了网络变化的开销，方便网络的维护和管理；
- 增加组网的灵活性，建立不受物理位置限制的具有一定独立性的 VLAN；
- 有效隔离 VLAN 间广播，防止网络的广播风暴；
- 可以有效地管理和限制 VLAN 间的访问，减少路由开销；
- 增加网络内部的安全性。

5.2.2 VLAN 的划分方法

VLAN 建立在交换技术的基础上，通过交换机“有目的地”发送数据，灵活地进行逻辑子网（广播域）的划分，而不像传统的局域网那样把站点束缚在所处的物理网络之中。

划分 VLAN 的方式有多种，每种方法的侧重点不同，所达到的效果也不尽相同。下面介绍几种划分方法。

1．根据端口划分 VLAN

这是应用最广泛、最有效的一种 VLAN 划分方法，目前绝大多数使用 VLAN 协议的交换机都提供这种 VLAN 配置方法。这种划分 VLAN 的方法是根据以太网交换机的交换端口来划分的，它将 VLAN 交换机上的物理端口和其内部的 PVC（永久虚电路）端口分成若干个组，每个组中被设定的端口都在同一个广播域中，构成一个虚拟网。通过交换机的端口定义，可以将连接在一台交换机上的站点划分为不同的子网，在图 5.8（a）中，将与端口 1、2、3、7、8 连接的计算机定义为 VLAN1，将与端口 4、5、6 连接的计算机定义为 VLAN2；也可以将连接在不同交换机上的站点划分在一个子网中；在图 5.8（b）中，将与交换机 1 的端口 1、2、3 和与交换机 2 的端口 4、5、6、7 连接的计算机定义为 VLAN1，将与交换机 1 的端口 4、5、6、7、8 和与交换机 2 的端口 1、2、3、8 连接的计算机定义为 VLAN2。

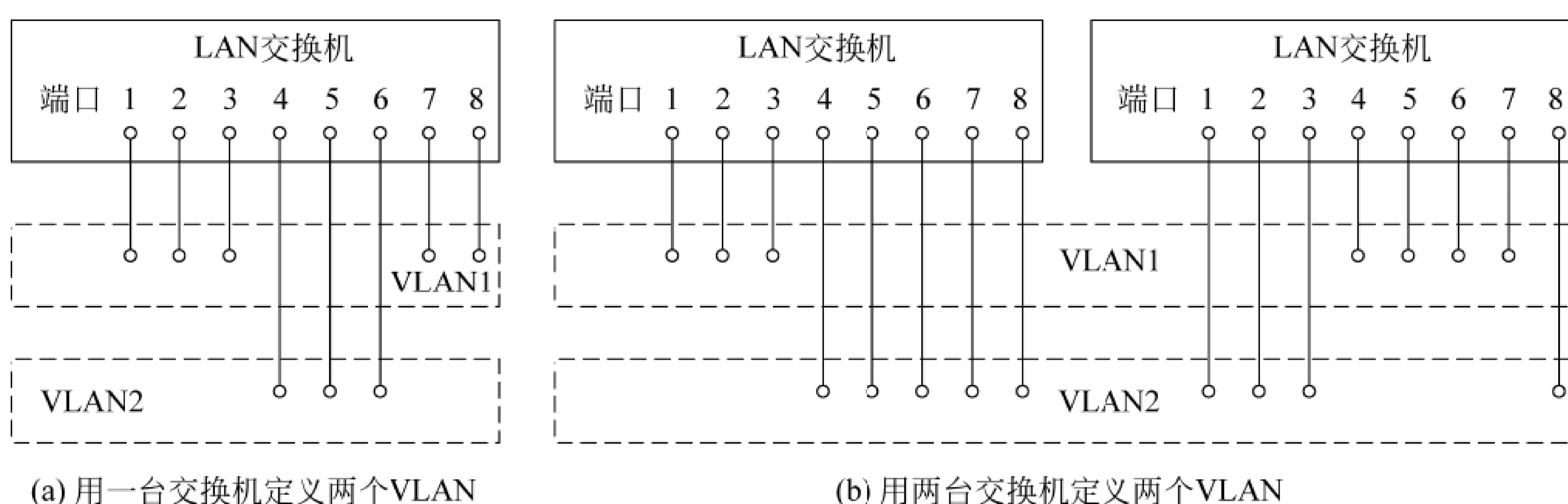


图 5.8　端口定义 VLAN

从这种划分方法本身可以看出，定义端口 VLAN 成员时非常简单，只要将所有的端口都定义为相应的 VLAN 组即可，适合于任何大小的网络。它的缺点是不允许多个 VLAN 共享一个物理网段或交换机端口。如果某一用户从一个端口所在的虚拟网移动到另一个端口所在的虚拟网，网络管理员需要重新进行设置。

2．根据 MAC 地址划分 VLAN

MAC VLAN 是根据每个主机的 MAC 地址来划分的。其优点是允许工作站移动到网络

的其他物理网段中。因为 MAC 地址是与硬件相关、固定于工作站的网卡内的，当网络用户从一个物理位置移动到另一个物理位置时，VLAN 交换机将跟踪属于 VLAN 的 MAC 地址，自动保留其所属 VLAN 的成员身份。

MAC VLAN 的不足之处在于所有的用户必须被明确地分配给虚拟网，要求所有用户在初始阶段必须配置到至少一个 VLAN 中；初始配置必须由人工完成，然后才可以自动跟踪用户。这对于用户较多的大型网络是非常烦琐的。

3．基于网络层协议划分 VLAN

基于网络层协议划分的 VLAN 也称第三层 VLAN，是按网络层协议，如 IP、IPX、DECnet、AppleTalk、Banyan 等划分 VLAN。这种方法的优点是用户的物理位置改变了，不需要重新配置所属的 VLAN，这对网络管理者来说很重要。这种划分方法由于不需要附加的帧标签来识别 VLAN，可以减少网络的通信量。

这种方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的（相对于前面两种方法），一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片能检查 IP 帧头，需要更高的技术，同时也更费时。当然，这与各个厂商的实现方法有关。

这种按网络层协议来组成的 VLAN，可使广播域跨越多个 VLAN 交换机。这对于希望针对具体应用和服务来组织用户的网络管理员来说是非常具有吸引力的，用户可以在网络内部自由移动，但其 VLAN 成员身份仍然保留不变。

4．按策略划分 VLAN

基于策略组成的 VLAN 能实现多种分配方法，包括 VLAN 交换机端口、MAC 地址、IP 地址、网络层协议等。网络管理人员可根据自己的管理模式和本单位的需求来决定选择哪种类型的 VLAN。

5．其他划分方法

（1）利用 IP 广播域来划分 VLAN。利用 IP 广播域来划分虚拟网的方法给使用者带来了巨大的灵活性和扩展性。在这种方式下，整个网络可以非常方便地通过路由器或第三层交换机扩展网络规模。

（2）按用户定义、非用户授权划分 VLAN。为了适应特别的 VLAN 网络，根据具体的网络用户的特别要求来定义和设计 VLAN，而且可以让非 VLAN 群体用户访问 VLAN，但是需要提供用户密码，在得到 VLAN 管理的认证后才可以加入一个 VLAN。

5.3　无线局域网

无线局域网（Wireless Local Area Network，WLAN）是以无线方式相连的计算机之间的资源共享，它除具有传统网络所支持的各种服务功能外，还可以在一定的区域实现移动并随时与网络保持联系。通常在下列 3 种情形下可能需要使用无线局域网：

- 无固定工作场所的使用者；
- 有线局域网络架设受环境限制；
- 作为有线局域网络的备用系统。

5.3.1　WLAN 的传输介质

与有线网络一样，无线局域网同样也需要传输介质。只是无线局域网采用的传输媒体不是双绞线或者光纤，而是红外线（IR）或者无线电波（RF），以后者使用居多。

采用无线电波作为传输介质是目前无线局域网的主流。它使用的频段主要是 S 频段（2.4～2.4835GHz）。这个频段也叫 ISM（Industry Science Medical），即工业科学医疗频段。该频段在美国不受美国联邦通信委员会（Federal Communications Commission，FCC）的限制，属于工业自由辐射频段，不会对人体健康造成伤害。所以无线电波成为无线局域网最常用的无线传输媒体。

如表 5.4 所示为在 WLAN 中使用的无线频段范围与其他物理参数。

表 5.4　WLAN 介质物理参数

频　段	亚微米（1～3GHz）		亚毫米（10～30GHz）	红　　外		
传输技术	窄带调制	扩展频谱	窄带调制	定向波束红外线（DB/IR）方式		扩散红外线（DF/IR）方式
				点对点方式	反射方式	
传输速度	几百千比特每秒～10Mbps		>100Mbps	可达 50Mbps	可达 10Mbps	几十千比特每秒～10Mbps
通信距离	100m（无须视距）		几十米（无须视距）	>50m（视距）	—（无须视距）	数米～20m（无须视距）
移动支持	一般	好	一般	不支持	不支持	差
成　　本	低	高	高	高	高	低
使用许可	需要	ISM 频段不需要	需要	不需要	不需要	不需要

从表中可以看出，目前 WLAN 的传输速率可以从几百千比特每秒至几十兆比特每秒。

5.3.2　无线局域网的结构

1. WLAN 的有关概念

1）工作站

连接在无线局域网中的工作站按照移动性可以分为两类。

- 固定站：如台式计算机和其他有线局域网中的设备。
- 移动站：在移动过程中也需要与网络通信的站，如手机、笔记本电脑等。

2）基本服务集

IEEE 制定的 WLAN 的协议标准是 IEEE 802.11。IEEE 802.11 规定 WLAN 的最小构件是基本服务集（Basic Service Set，BSS）。BSS 所覆盖的地理范围称为一个基本服务区（Basic Service Area，BSA）。按照 IEEE 802.11 规定，一个 BSS 中包括一个基站和若干移动站。

3）接入点

按照 IEEE 802.11 规定，BSS 中的基站称为接入点（Access Point，AP）。所以 BSA 也是 AP 的覆盖范围。AP 承担 BSA 中的无线通信管理及与其他网络（包括其他 BSS 以及有线网络）的连接工作，组成扩展服务集（Extended Service Set，ESS），如图 5.9 所示。

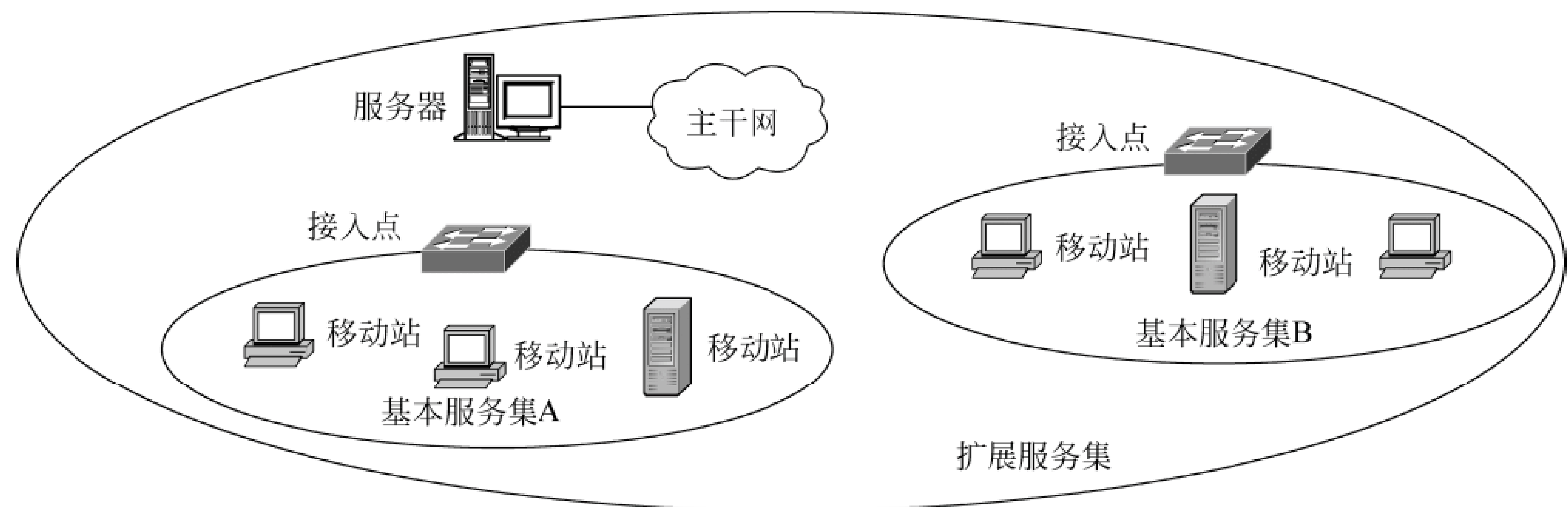


图 5.9　扩展服务集

2．WLAN 的结构

无线局域网可以在普通局域网的基础上通过无线 Hub、无线接入站（AP）、无线网桥、无线 Modem、无线网卡等实现，并形成不同的网络结构。

1）基站接入的独立 WLAN

这是一种采用移动蜂窝通信网接入方式组建 WLAN 的方式。如图 5.10 所示，在这种方式下，各站点之间是通过基站接入、交换数据、互相连接。利用这种方式，可以实现各移动站通过交换中心的自组网，还可以通过广域网远地站点组建自己的工作网络。

2）无中心独立 WLAN

如图 5.11 所示，无中心结构允许网中任意两个站点间直接通信，是一种分布式对等结构方式。这种结构的缺点是各用户之间的通信距离较近，且当用户数量较多时，性能较差。

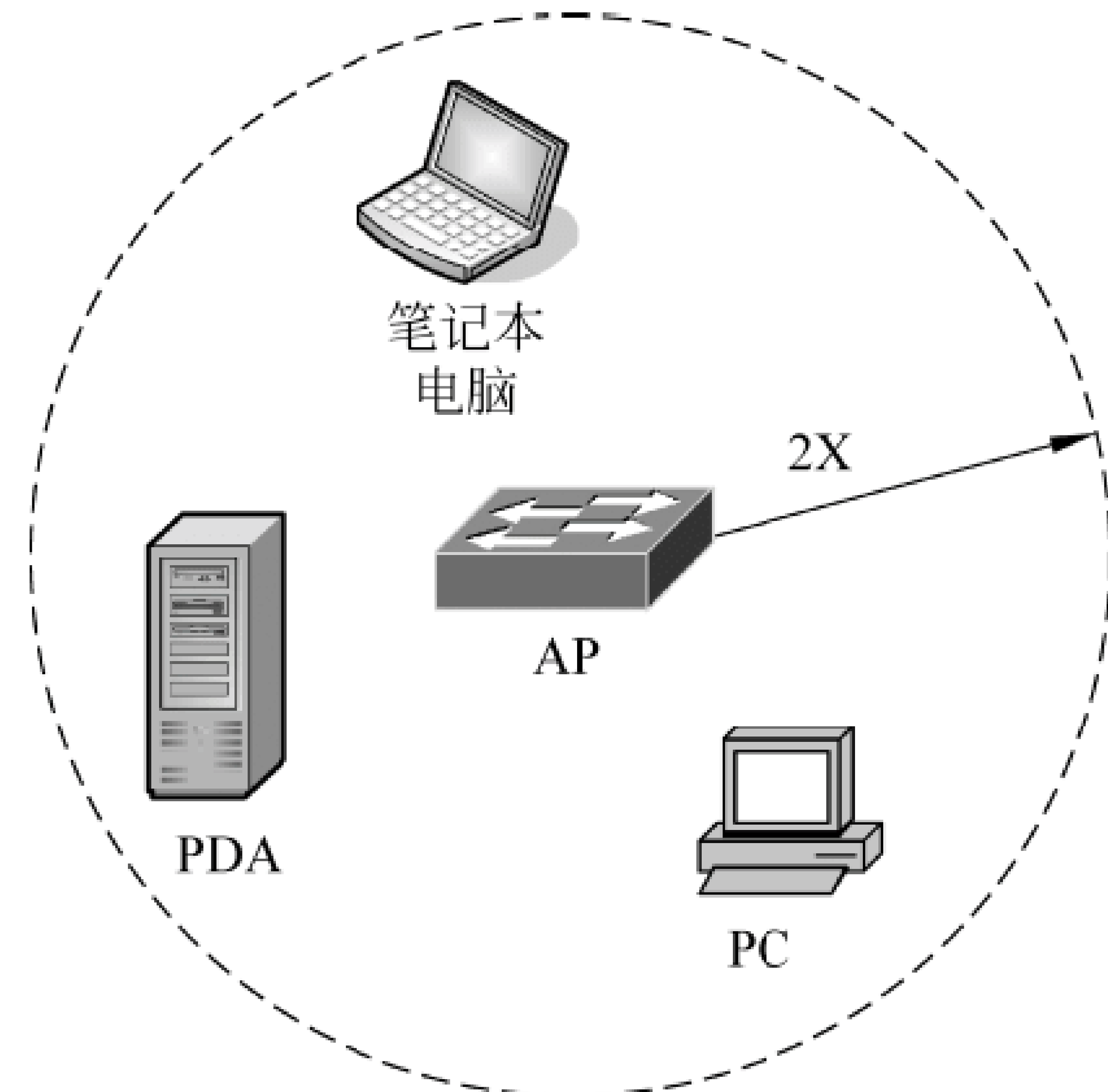


图 5.10　基站接入的独立 WLAN

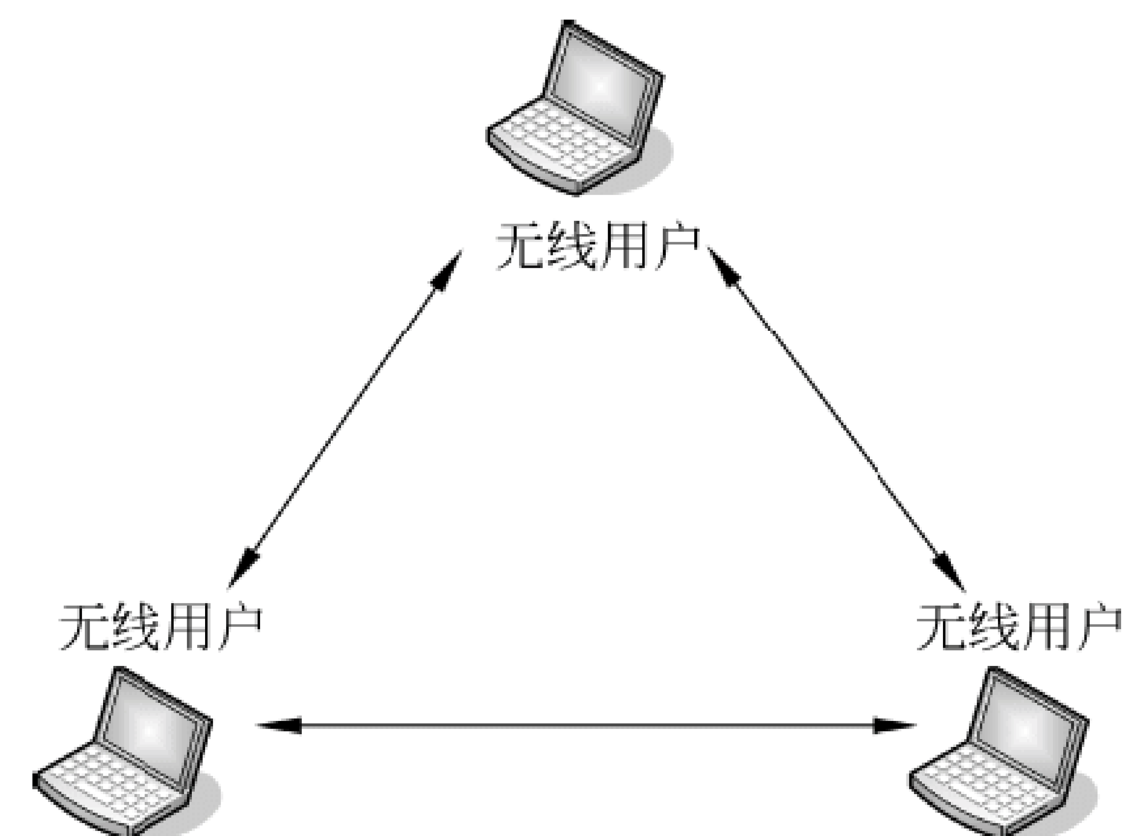


图 5.11　无中心独立 WLAN

3）非独立的 WLAN

当无线通信作为有线通信的一种补充和扩展时，称为非独立的 WLAN。如图 5.12 所示，在这种配置下，多个 AP 通过线缆连接在有线网络上，以使无线用户能够访问网络中的各个

部分。

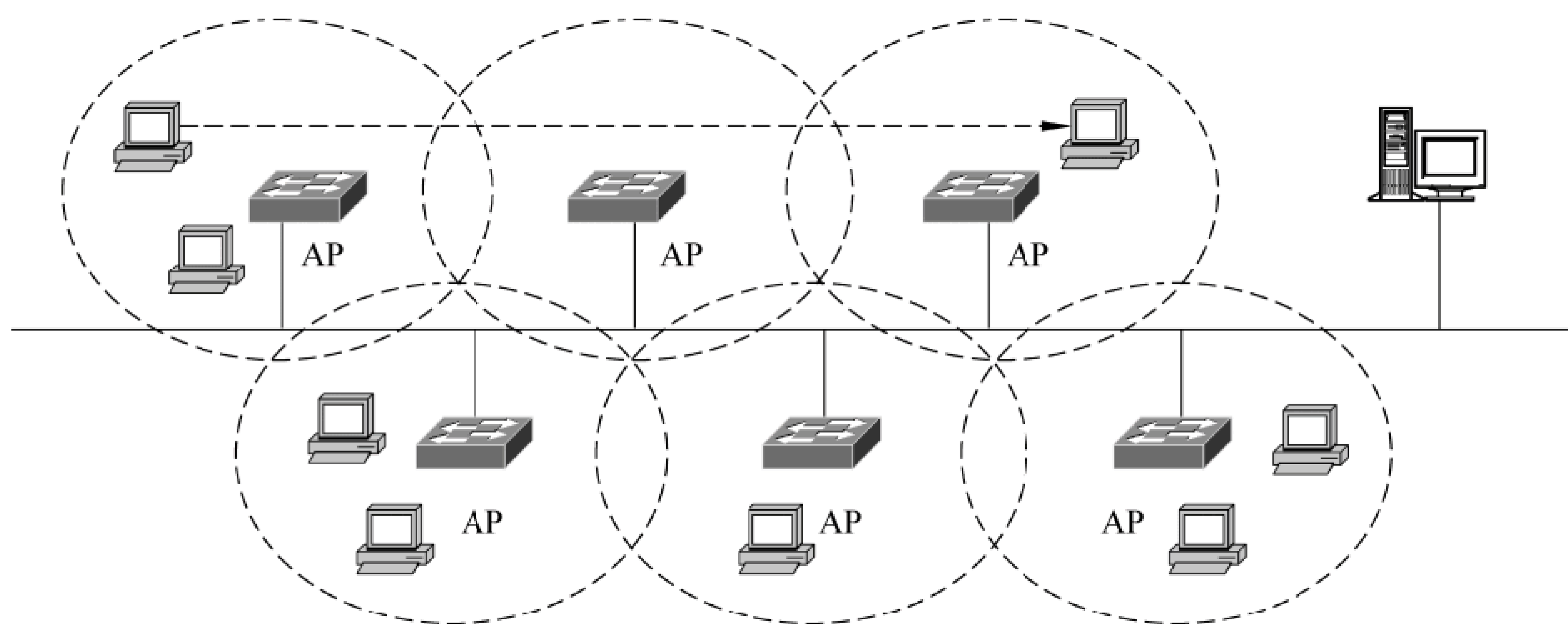


图 5.12　非独立的 WLAN

5.3.3　IEEE 802.11 协议

IEEE 802 委员会的 802.11 工作委员会成立于 1990 年 7 月，1998 年完成 802.11 的制定工作。它的标准化也主要表现在 LLC 以下即 MAC 层和物理层。

1．物理层

IEEE 802.11 协议定义了 WLAN 所使用的无线频段以及调制方式，并进一步分为 802.11、802.11b 和 802.11a 三种类型。

（1）IEEE 802.11 使用 2.4GHz 频带，传送速率为 1Mbps。

（2）IEEE 802.11b 使用 2.4GHz 频带，标称传送速率为 11Mbps，实际为 7～8Mbps。

（3）IEEE 802.11a 使用 5GHz 频带，传送速率为 54Mbps。

2.4GHz 频带是一个容易受微波炉、无绳电话和其他无线设备干扰的频带，5GHz 频带是一个干扰较小的频带。

WLAN 的 3 种主要物理层实现方法是跳频扩频（Frequency-Hopping Spread Spectrum，FHSS）、直接序列扩频（Direct Sequence Spread Spectrum，DSSS）和红外（IR）。

红外方式使用波长为 850～950nm 的红外线传送数据，速率为 1～2Mbps。

2．MAC 层

从原则上讲，IEEE 802.11 的 MAC 层协议与有线局域网的 MAC 协议并无本质上的区别。图 5.13 中给出了 IEEE 802.11 的 MAC 层结构，称为 DFWMAC（分布式基础无线网 MAC）。它可以为本地链路控制层提供竞争服务和无竞争服务。

1）竞争服务

在有竞争的情况下，WLAN 像以太网一样，用载波侦听的方法将访问介质的决定发布到每个结点。但是，由于在无线局域网上信号的动态范围很广，发送站难于有效地识别是噪声还是自己发送的信号，因而要检测冲突不现实，无法沿用原有的 CSMA/CD，而是采用了带有冲突避免的载波多路侦听协议 CSMA/CA 作为 MAC 层的协议。

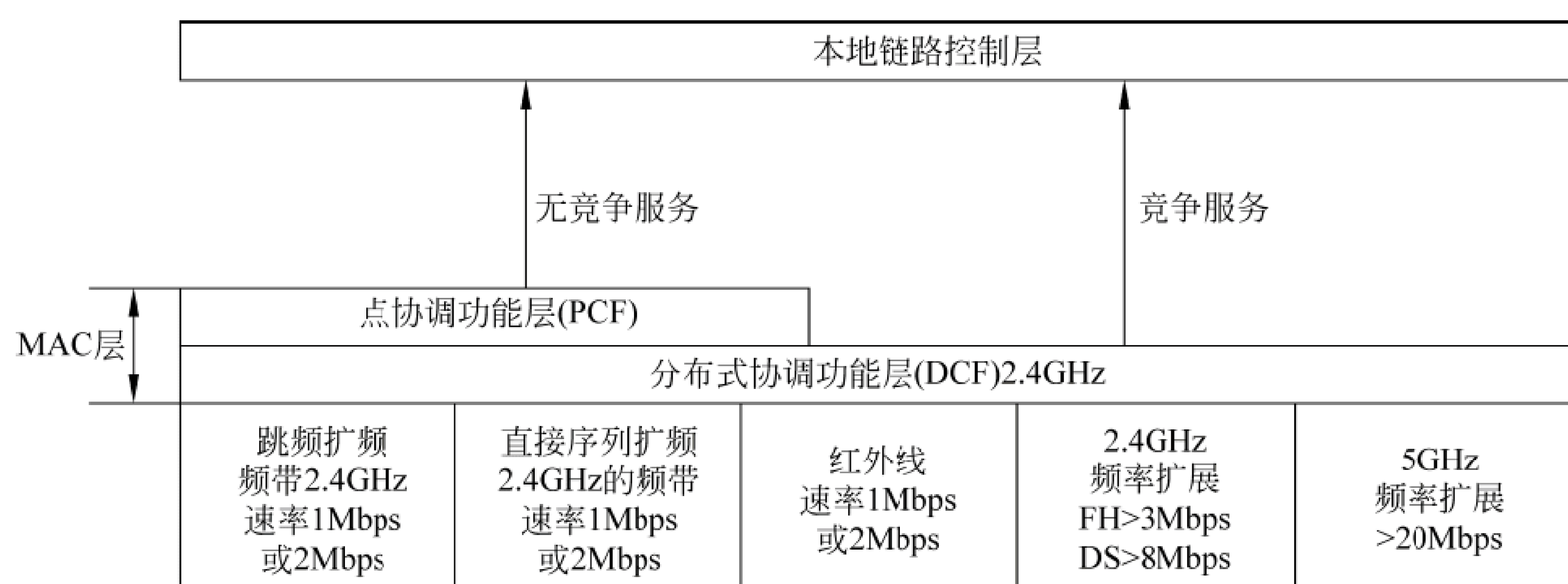


图 5.13　IEEE 802.11 协议结构

CSMA/CA 并不能完全避免冲突，但可以减少碰撞几率。如图 5.14 所示，CSMA/CA 的访问规则如下。

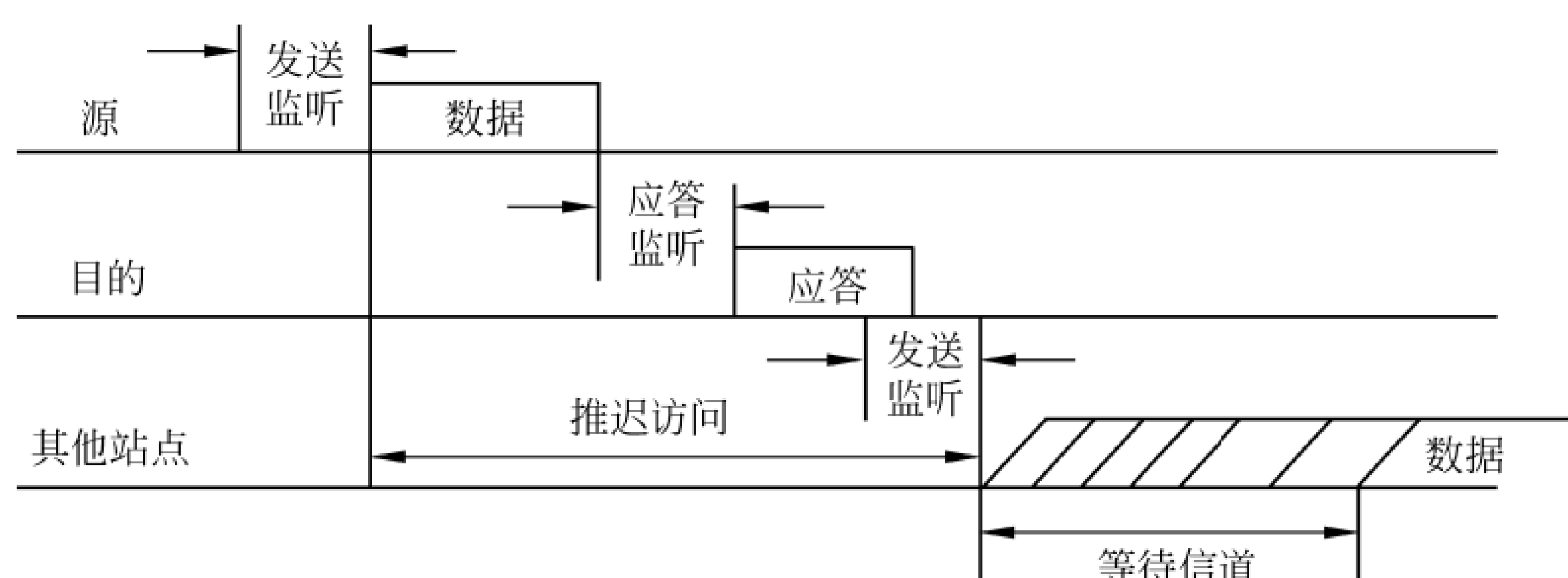


图 5.14　发送站点使用 IFS 的 CSMA 访问规则

（1）任何一个站点在发送数据之前，要先监听载波，确认信道空闲时，发送探询帧，仅当信道空闲一个 IFS（Inter-Frame Space，帧间隙）的时间后仍然空闲，才发送数据。

（2）如果介质忙（包括侦听中发现忙、在 IFS 时间内发现忙），站点要推迟一个随机时间后重新尝试。

（3）一旦当前的数据传送完毕，站点要再延迟一个 IFS 时间；如果在这段时间内介质仍然忙，站点就使用二进制退避算法并继续监听介质，直到介质空闲。

（4）接收端在收到数据后，等信道空闲一个 IFS 时间后才发出回答帧，否则推迟一个随机时间后重新尝试。

2）无竞争服务

无竞争服务采用集中访问控制，包括集中轮询主管的轮询，由一个中央的决策者协调访问请求，实现可以选择的访问——点协调功能（Pointer Coordination Function，PCF）。这种机制适合于下列情形：

- 几个互连的 WLAN；
- 一个与有线主干网相连的基站；
- 实时性强的点；
- 高优先级的站点。

PCF 在分布式协调功能（Distributed Coordination Fuction，DCF）的顶部实现，它在发出轮询时使用 PIFS（PCF IFS），将所有异步帧都排除在外，并使优先级高的站点可以先

发送。

5.3.4 蓝牙技术

1. 蓝牙技术概述

蓝牙是一种支持点到点、点到多点的语音、数据业务的短距离无线通信技术方案，也是一种大容量近距离无线数字通信的技术标准，其目标是实现最高数据传输速度 1Mbps（有效传输速率为 721kbps）、传输距离为 10cm～10m，通过增加发射功率可达到 100m。

“蓝牙”最先由爱立信（Ericsson）、诺基亚（Nokia）、英特尔（Intel）、IBM 和东芝（Toshiba）5 家公司于 1995 年提出，后来又有 3COM、朗讯（Lucent）、摩托罗拉（Motorola）、微软（Microsoft）加入，9 家公司组成蓝牙特殊兴趣小组（Bluetooth Special Internet Group，BSIG）发起并制定取代数据电缆的短距离无线连接技术标准，并在 1999 年 7 月 26 日推出了蓝牙技术规范的 1.0 版本，2001 年 2 月 22 日推出了 1.1 版本。蓝牙兴趣小组采取了无偿向全世界产业界转让该项专利技术的策略，迅速得到全世界 2 000 多家企业加盟，IEEE 也专门成立了 IEEE 802.15 小组负责研究基于蓝牙的 PAN 技术，目前不断有蓝牙技术的电子产品问世。

2. 蓝牙技术要点

下面先介绍蓝牙技术中的几点主要技术。

1）采用 ISM 频段

ISM（Industrial Scientific Medical）频段，分为工业（902～928MHz）、科学研究（2.42～2.4835GHz）和医疗（5.725～5.850GHz），由美国联邦通信委员会（FCC）分配的不必许可证的无线电频段（功率不能超过 1W）。1997 年 1 月核准用于无线局域网（WLAN）的是医疗频段。

2）跳频扩频调制技术

蓝牙把 2.4GHz 的 ISM 频段分割成 79 个信道频道可供跳频使用，第一个频道的中心频率为 2.402GHz，以后每隔 1MHz 为一个信道，并以每秒 1600 次的伪随机跳频波形在其间改变频率，形成总带宽很宽，但瞬时带宽很窄而跳频速度很高的一些信道，其抗干扰性和链路的安全可靠性都很好。

蓝牙的信道采用 FH/TDD（跳频/时分）复用结构，每个时隙用不同的跳频信号传输一个数据分组。连续的时隙在发送和接收中交替使用，形成时分复用结构。

一般说来，在一个跳频系统中，遇到干扰的每一跳都会丢失该跳期间所发送的数据分组。对蓝牙系统来说，79 个信道每跳变一次仅丢失一个分组。这也证明了蓝牙技术在抗干扰方面的优势。

3）微微网结构

微微网以 3bit 地址来区分微微网中的设备，这个地址称为微微网的 MAC 地址。

微微网中所有的设备都是级别相同、具有相同权限的工作单元。但是，在微微网初建

时，有一个单元会被指定为主工作单元（master unit），其时钟和跳频序列用于同步其他设备，其他工作单元被定义为从工作单元（slave unit）。

微微网可以采用点到点或点到多点的方式，由主工作单元将从工作单元连接起来。在同一微微网中，所有用户都用同一跳频序列同步。几个相互独立的、非同步的微微网，可以以特定方式连接在一起的微微网构成分布式的多微微网，称为散射网（scatternet）。各微微网由不同的跳频序列区分。如图 5.15 所示为几种可能的微微网拓扑结构。

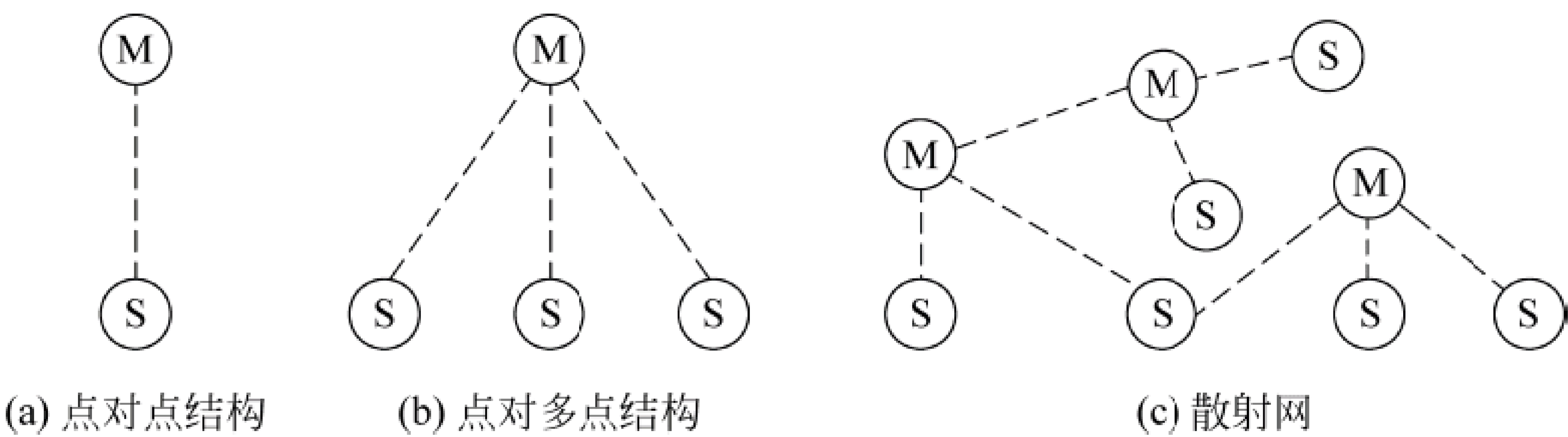


图 5.15　微微网的拓扑结构

4）低功耗工作方式

在微微网中，暂不进行数据传输的单元将转入节能工作方式。按照节能能力，低功耗工作方式可依次分为监听方式（sniff mode）、保持方式（hold mode）和休眠方式（parked mode）。

（1）监听方式。在监听方式下，从工作单元的监听时间间隔增大，其间隔大小视应用情况，可由程序设定。

（2）保持方式。在保持方式下，只有内部定时器工作。工作单元由保持方式转出后，即可恢复数据传送。从工作单元可以由主工作单元设置为保持方式，也可以自己要求转入保持方式。

（3）休眠方式。在休眠方式下，工作单元放弃 MAC 地址，仅偶尔监听网络的同步信号和检查广播信号。

3. 蓝牙系统结构

蓝牙系统的基本单元由天线射频单元、连接控制单元（基带模块）、存储底层协议的存储器、主机接口等组成，其结构如图 5.16 所示。

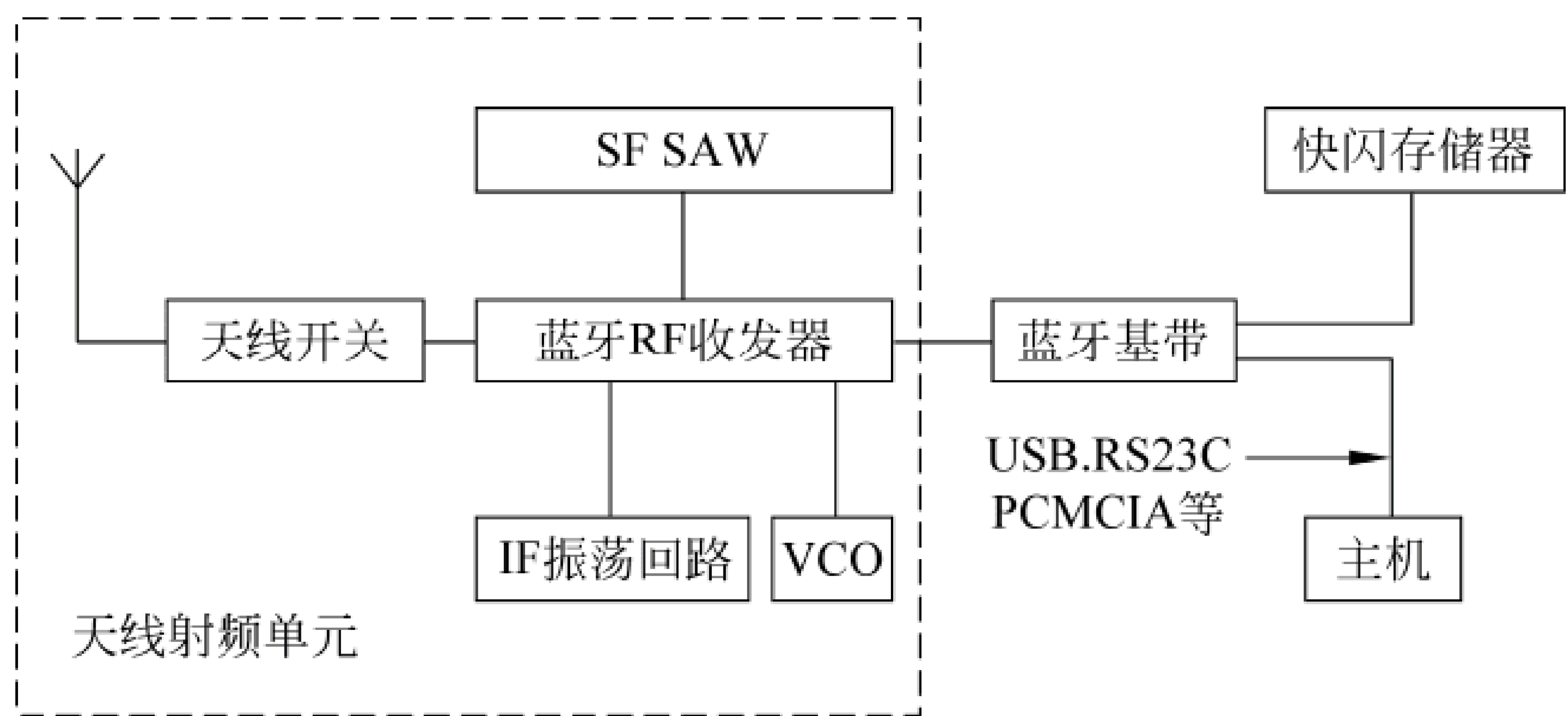


图 5.16　蓝牙系统结构

天线射频（Radio Frepuency，RF）单元包括完整的无线跳频发射和接收部分，实现数

据位流的过滤和传输。天线的发射功率要符合 FCC 关于 ISM 波段的要求。在 RF 输入级采用高 Q 值陶瓷或表面声波（Surface Acoustic Wave，SAW）滤波器，以抑制 GSM 发射机产生的阻塞信号。VCO 为压控振荡器（Voltag Controlled Dscillator）。

连接控制单元，即带处理器的蓝牙基带（bluetooth baseband，BB）描述了数字信号的硬件部分——链路控制器，用于实现基带协议和其他底层协议。

5.3.5 Wi-Fi

1. Wi-Fi 概述

Wi-Fi（Wireless Fidelity，无线保真）是一种可以将个人 PC、手持设备（如 pad、手机）等终端以无线方式互相连接的技术。事实上它是一个高频无线电信号，也是一个无线网络通信技术的品牌，还是一种商业认证，同时也是一种无线联网技术。它由澳洲政府的研究机构 CSIRO 在 20 世纪 90 年代发明并于 1996 年在美国成功申请了无线网技术专利（U.S. Patent Number 5,487,069），发明者是由悉尼大学工程系毕业生组成的研究小组，领导人是 Dr. John O'Sullivan。

2. Wi-Fi 技术标准

John O'Sullivan 领导的 Wi-Fi 研究小组的初衷是改善基于 IEEE 802.11 标准的无线网路产品之间的互通性。目前已经有了四级 Wi-Fi 技术标准，形成了一个不同级别的技术标准簇。如表 5.5 所示，每一级标准都给出了这类产品应当具有的技术性能、频率、带宽特性定义。将来还会有更新的标准出台，更加详细地定义 WI-Fi 的新特性、安全性和其他性能。Wi-Fi 都要贴上相应的 IEEE 802.11 标签，表明该产品满足所有标识上注释的标准。

表 5.5　已有的 Wi-Fi 标准簇

标准号	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g	IEEE 802.11n
标准发布时间	1999 年 9 月	1999 年 9 月	2003 年 6 月	2009 年 9 月
工作频率范围	2.4～2.4835GHz	5.150～5.350GHz 5.475～5.725GHz 5.725～5.850GHz	2.4　～2.4835GHz	2.4～2.4835GHz 5.150～5.850GHz
非重叠信道数	3	24	3	15
物理速率（Mbps）	11	54	54	600
实际吞吐量（Mbps）	6	24	24	100 以上
频宽	20MHz	20MHz	20MHz	20MHz/40MHz
调制方式	CCK/DSSS	OFDM	CCK/DSSS/OFDM	MIMO-OFDM/DSSS/CCK
兼容性	IEEE 802.11b	IEEE 802.11a	IEEE 802.11b/g	IEEE 802.11a/b/g/n

3. Wi-Fi 信道

IEEE 802.11b/g 标准工作在 2.4GHz 频段，频率范围为 2.400～2.4835GHz，共 83.5MHz 频宽，划分为 14 个子信道，每个子信道宽度为 22MHz，相邻信道的中心频点间隔 5MHz，

如图 5.17 所示。中国划分为 13 个信道，每个信道带宽为 22MHz。

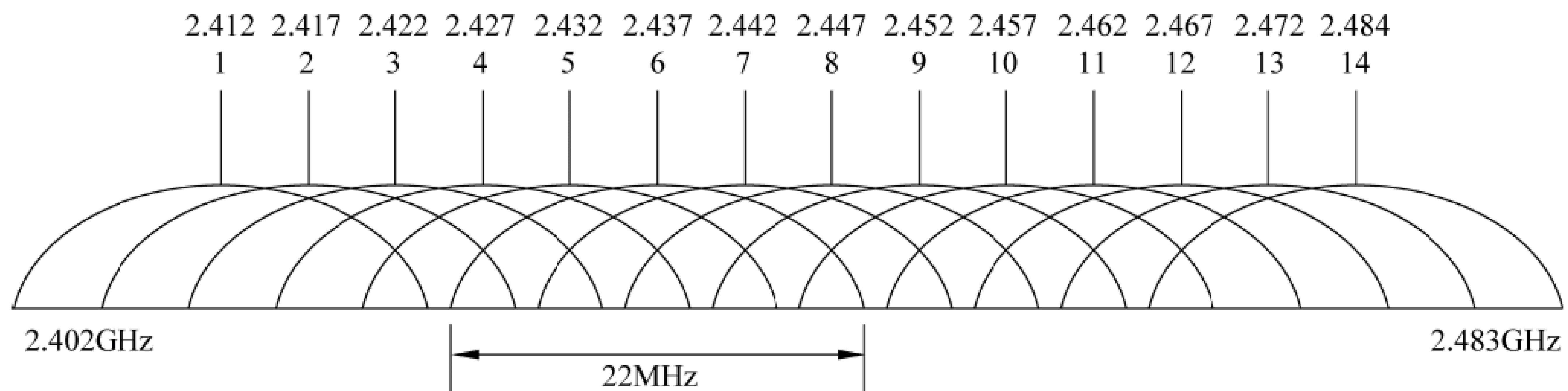


图 5.17　IEEE 802.11b/g 信道

各个国家在信道的具体划分上略有差异：

- 北美/FCC　2.412～2.461GHz（11 信道）。
- 欧洲/ETSI　2.412～2.472GHz（13 信道）。
- 日本/ARIB　2.412～2.484GHz（14 信道）。
- 中国划分为 13 个信道，每个信道带宽为 22MHz。

4. 服务集和 Wi-Fi 的工作过程

一个 AP 可以向进入其覆盖范围的 STA（工作站，station）提供一个移动到一个服务集（Service Set，SS）。每个 AP 所提供的 SS 由其 SSID 标识。Wi-Fi 的工作过程，就是客户端按照 SSID 与符合的 AP 之间的通信过程，包括扫描、接入、认证、加密、漫游和同步等功能。

这些工作主要由 IEEE 802.11MAC 层负责。

5. 无线接入过程

如图 5.18 所示，STA 启动初始化、开始正式使用 AP 传送数据帧前，要经过三个阶段才能够接入：

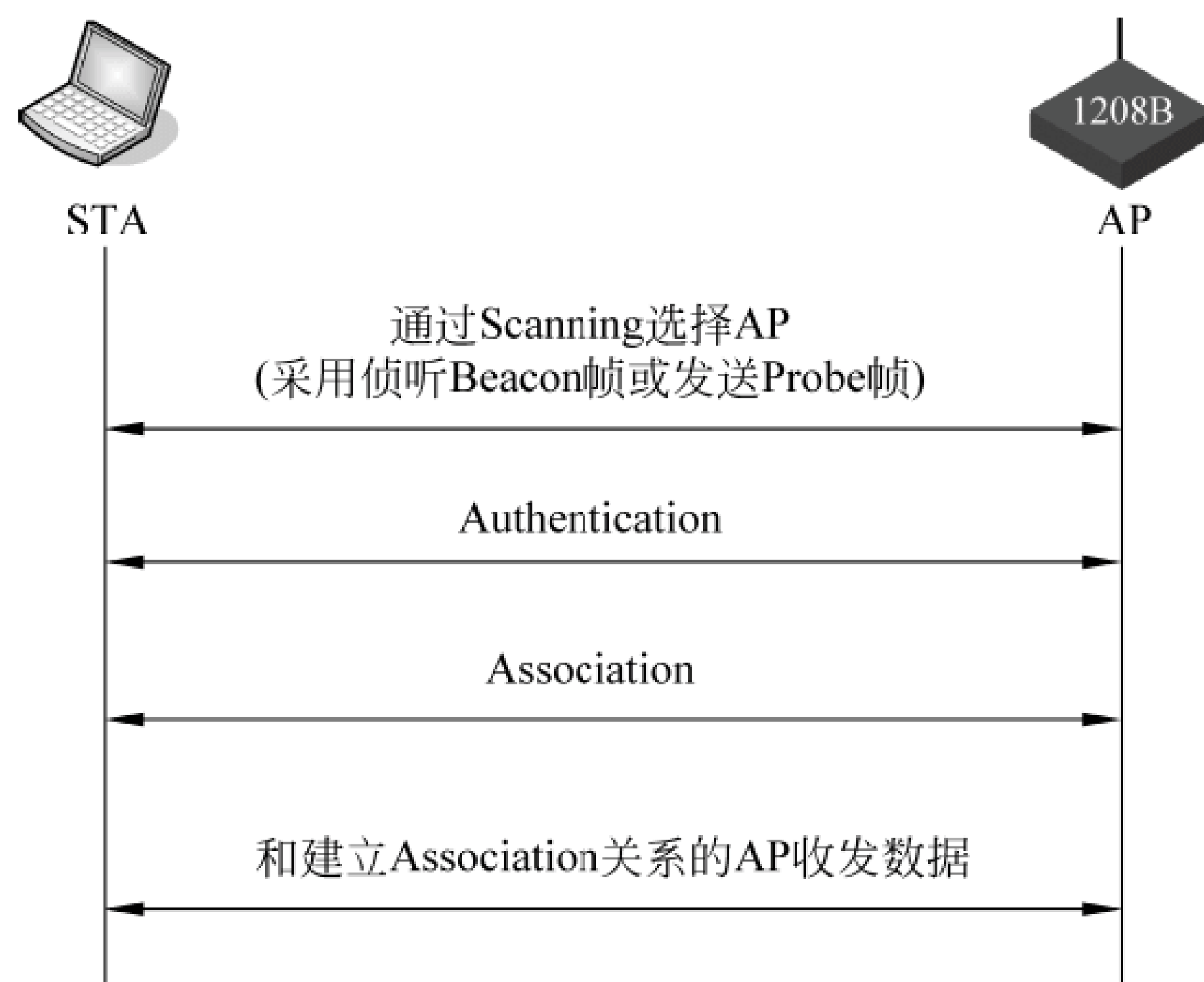


图 5.18　无线接入过程

- 扫描阶段（Scanning）。

- 认证阶段（Authentication）。
- 关联（Association）。

1）扫描阶段（Scanning）

当 STA 漫游时，要寻找连接一个可以连接的 AP。STA 会在每个可用的信道上进行搜索。搜索用扫描的方式进行，IEEE 802.11 MAC 提供了如下两种扫描方式。

（1）被动扫描（passive scanning）：通过侦听 AP 定期发送的 Beacon（指引）帧来发现网络，该帧提供了 AP 及所在 SS 相关信息："我在这里……"。这种扫描找到时间较长，但 STA 节电。

（2）主动扫描（active scanning）：STA 依次在 13 个信道发出 Probe Request（搜索请求）帧，寻找与符合 SSID 指定的 AP；若找不到相同 SSID 的 AP，则一直扫描下去。这种扫描可以能迅速找到。

2）认证阶段（Authentication）

当 STA 找到 SSID 匹配的 AP 后，会根据收到的 AP 信号强度，选择一个信号最强的 AP，然后进入认证阶段。只有通过身份认证的站点才能进行无线接入访问。AP 提供如下认证方法：

- 开放系统身份认证（open-system authentication）。
- 共享密钥认证（shared-key authentication）。
- WPA PSK 认证（pre-shared key）。
- 802.1X EAP 认证。

3）关联（Association）

AP 向 STA 返回认证响应信息，身份认证获得通过后，进入关联阶段：先由 STA 向 AP 发送关联请求，再由 AP 向 STA 返回关联响应。

至此，接入过程才完成，STA 初始化完毕，可以开始向 AP 传送数据帧。图 5.19 描述了在一个区间内有两个 AP 时，用户初始化连接到一个 AP 的过程。

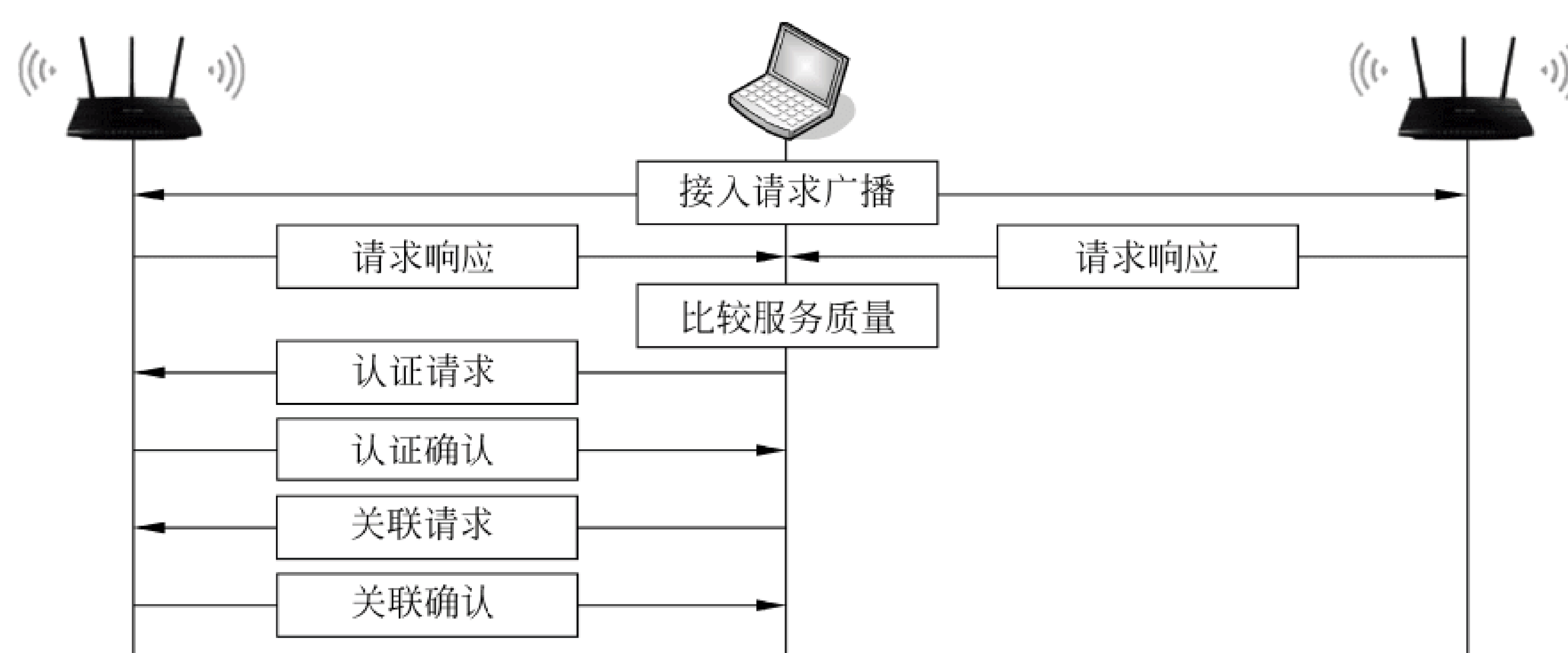


图 5.19　STA 初始化连接到一个 AP 的过程

5.3.6　ZigBee

随着移动个人局域网和工业自动化技术的发展，展示出日益扩展在短距离、低功耗无线技术市场。1999 年，蓝牙热潮席卷全球，然而发展数年，人们发现蓝牙用于工业自动化并不理想，受技术复杂、价格偏高、组网规模太小、抗干扰能力差等问题的困扰，一部分

人便另起炉灶，致力于开发一种低成本、低功耗、高可靠性的短距离无线传输技术。

ZigBee 又称紫蜂协议，这一名称来源于蜜蜂的八字舞。因为蜜蜂（bee）是靠飞翔和“嗡嗡”（zig）地抖动翅膀的“舞蹈”来与同伴传递花粉所在方位和远近信息的，也就是说，蜜蜂依靠着这样的方式构成了群体中的通信“网络”，因此 ZigBee 的发明者们说，利用蜜蜂的这种行为来形象地描述这种无线信息传输技术。下面进一步分析其技术特点。

（1）工作方式特点。ZigBee 协议从下到上分别为物理层(PHY)、媒体访问控制层(MAC)、传输层(TL)、网络层(NWK)、应用层(APL)等。其中物理层和媒体访问控制层遵循 IEEE 802.15.4 标准的规定。其工作频段为：2.4GHz （全球）、915MHz（美国）和 868MHz（欧洲）。这几个频段是免执照频段。

由于此三个频带物理层并不相同，其各自信道带宽也不同，分别为 0.6MHz、2MHz 和 5MHz。分别有 1 个、10 个和 16 个信道。

这三个频带的扩频和调制方式亦有区别。扩频都使用直接序列扩频(DSSS)，但从比特到码片的变换差别较大。调制方式都用了调相技术，但 868MHz 和 915MHz 频段采用的是 BPSK，而 2.4GHz 频段采用的是 OQPSK。

（2）低速率。ZigBee 的三个频带分别提供为 250kbps(2.4GHz)、40kbps(915MHz)和 20kbps(868MHz)的原始数据吞吐率。所以最高传播速率只有 250kbps，而且这只是链路上的速率，除掉信道竞争应答和重传等消耗，真正能被应用所利用的速率可能不足 100kbps，并且余下的速率可能要被邻近多个结点和同一个结点的多个应用所瓜分，因此不适合做视频之类事情，只适合工业自动化控制以及物联网中的数据传输。

（3）低功耗。由于 ZigBee 结点所承载的应用数据速率都比较低，因此在不需要通信时，结点可以进入很低功耗的休眠状态，此时能耗可能只有正常工作状态下的千分之一。由于一般情况下，休眠时间占总运行时间的大部分，有时正常工作的时间还不到百分之一，因此能取得很好的节能效果。据测试，在低耗电待机模式下，2 节 5 号干电池可支持 1 个结点工作 6～24 个月，甚至更长。相比之下，蓝牙可以工作数周，Wi-Fi 则只可以工作数小时。

（4）低成本。ZigBee 通过大幅简化协议（不到蓝牙的 1/10），降低了对通信控制器的要求，按预测分析，以 8051 的 8 位微控制器测算，全功能的主结点需要 32KB 代码，子功能结点少至 4KB 代码，而且 ZigBee 免协议专利费。每块芯片的价格大约为 2 美元。

（5）快响应。ZigBee 不需同步，因此结点加入网络和重新加入网络的过程很快，一般从睡眠转入工作状态只需 15ms，结点连接进入网络只需 30ms，进一步节省了电能。相比较，蓝牙需要 3～10s，Wi-Fi 需要 3s。但是，由于 ZigBee 采用随机接入 MAC 层，且不支持时分复用的信道接入方式，因此不能很好地支持一些实时的业务。

（6）高发射效率。在发射功率为 0dBm 的情况下，蓝牙通常能有 10m 的作用范围。而 ZigBee 在室内通常能达到 30～50m 的作用距离，在室外空旷地带甚至可以达到 400m（TI CC2530 不加功率放大）。因此说，ZigBee 传输范围一般介于 10～100m 之间，在增加 RF 发射功率后，亦可增加到 1～3km。这指的是相邻结点间的距离。如果通过路由和结点间通信的接力，传输距离将可以更远。

（7）高容量。ZigBee 可采用星状、片状和网状网络结构，由一个主结点管理若干子结点，最多一个主结点可管理 254 个子结点；同时主结点还可由上一层网络结点管理，最多

可组成 65 000 个结点的大网，而每个蓝牙网络只有 8 个结点。

（8）高可靠性。ZigBee 在很多方面提供了可靠性保证。

- 物理层采用了扩频技术，能够在一定程度上抵抗干扰。
- MAC 应用层(APS 部分)有应答重传功能。
- MAC 层的 CSMA 机制使结点发送前先监听信道，可以起到避开干扰的作用。
- 当 ZigBee 网络受到外界干扰，无法正常工作时，整个网络可以动态地切换到另一个工作信道上。
- ZigBee 采用蜂巢结构组网，每个设备不仅能通过多个方向与网关通信，保障网络的稳定性。
- 采用自组网和动态路由，自恢复能力强，可以在恶劣环境下保证数据传输的可靠性。

（9）高安全。ZigBee 提供了三级安全模式，包括无安全设定、使用接入控制清单（ACL）防止非法获取数据以及采用高级加密标准（AES128）的对称密码，以灵活确定其安全属性。

5.3.7　IPv6/6LoWPAN

20 世纪 80 年代末，在 Web 技术广泛应用中尝到的甜头，启发人们想把物体通过传感器互联起来。1990 年，施乐公司在其产品网络可乐贩售机（Networked Coke Machine）率先实现了这一设想。关于传感器网络（sensor network ）的研发迅速扩展开来，并在 1999 年人们又为其起了新的名称——Internet of things（IoT），中文被译成物联网，即物物相连的互联网。

物联网有两个重要条件：一是必然要采用无线技术，所以，ZigBee 以及类似标准如 z-wave、ANT、Enocean 等也先后出现；另一个条件是要借助互联网。但是，人们发现，由于 IP 技术过于复杂，不适合低功耗、资源受限的无线传感器网络（wireless sensor network），例如 ZigBee 需要接入互联网时需要复杂的应用层网关，也不能实现端到端的数据传输和控制。因此它们都是采用非 IP 技术。而且这些无线传感器网络技术之间相不兼容，不利于产业化的发展。

另一方面，物联网需要大量 IP 地址，又面临移动通信与个人组网对于 IP 地址需求的急剧增长，加剧了 IP 地址危机，导致目前的 IPv4 地址近乎枯竭。

IETF 和许多研究者发现了这些问题，决定把这些问题统一考虑。IETF 于 2004 年 11 月成立了一个 6LoWPAN 工作组，研究 IPv6 基于 IEEE 802.15.4 技术的无线传感器网络的关键问题，推出了 IPv6/6LoWPAN 协议。

Application protocols	
UDP	TCP
IPv6	
6LoWPAN	
IEEE 802.15.4 MAC	
IEEE 802.15.4 PHY	

图 5.20　6LoWPAN 协议栈

如图 5.20 所示，完整的 6LoWPAN 协议栈由物理层、介质访问控制层（MAC 层）、6LoWPAN 适配层、IPv6 网络层、传输层和高层应用规范组成。与 ZigBee 相同，6LoWPAN 技术底层采用 IEEE 802.15.4 规定的物理层和 MAC 层。

IPv6/6LoWPAN 具有诸多优势：可以运行在多种介质上，如低功耗无线、电力线载波、Wi-Fi 和以太网，有利于实现统一通信；IPv6 可以实现端到端的通信，无须网关，降低成本；6LoWPAN 中采用 RPL 路由协议，路由器可以休眠，也可以采用电池供电，应用范围广；而 ZigBee 技术路由器不能休

眠，应用领域受到限制；6LoWPAN 技术也具有自组织网络的特点，是物联网感知层、无线传感器网络的重要技术。6LoWPAN 标准已经得到大量开源软件（如最著名的 Contiki、TinyOS 等系统）实现，它们全部开源，完全免费，并在许多产品中得到应用。ZigBee 新一代智能电网标准 SEP 2.0 中也已经采用 6LoWPAN 技术。随着无线传感器网络的广泛应用，IPv6/6LoWPAN 协议将很可能成为该领域的事实标准。

实验 14　交换以太网的端口汇聚配置

一、概述

端口汇聚功能就是在交换机之间可以使用两条以上的链路进行级联，将平行的一组链路看作一条物理链路来增加交换机与交换机之间互联链路的带宽，并且实现链路备份。

本示例采用华为的 Quidway®S3026C-SIL2 线速以太网交换机设备（见图 5.21）。



图 5.21　Quidway®S3026C-SI

Quidway® S3026C-SI 以太网交换机提供固定的 24 个 10/100BASE-TX 的自适应端口、1 个 Console 口及 2 个扩展插槽，扩展插槽可支持百兆单模光模块、百兆多模光模块、百兆中距光模块、千兆电模块、千兆单模光模块、千兆多模光模块、千兆中距光模块、千兆长距光模块和堆叠模块，提供灵活的上行端口配置，可不依赖于其他设备独立运行。所有端口支持线速转发 12.8Gbps，交换容量包转发率 6.55Mbps。

图 5.22 为本例的端口汇聚配置的网络结构示意图。交换机 SwitchA 和 SwitchB 通过以太网口实现互连。SwitchA 用于互连的端口为 e0/1 和 e0/2，SwitchB 用于互连的端口为 e0/1 和 e0/2。

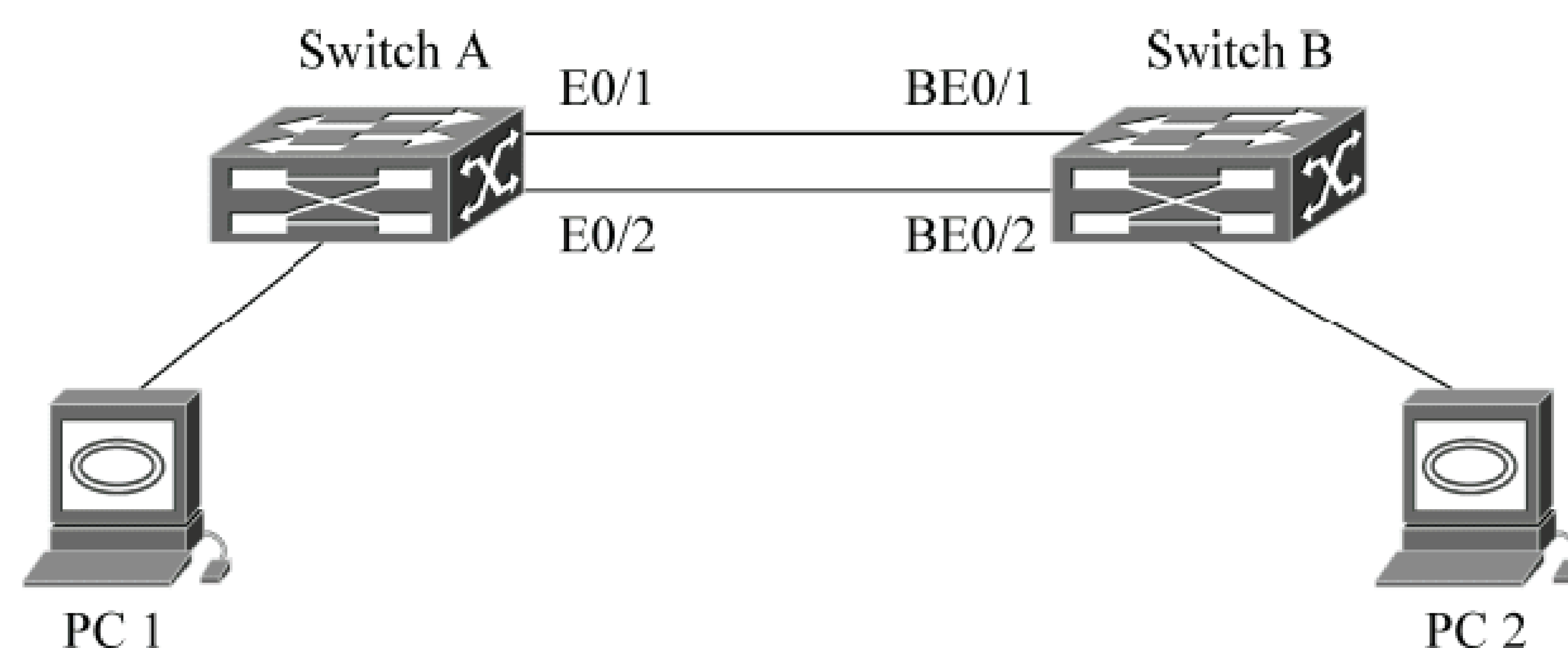


图 5.22　端口汇聚配置的网络结构

二、SwitchA 交换机配置步骤

（1）进入端口 E0/1

```
[SwitchA]interface Ethernet 0/1
```

（2）汇聚端口必须工作在全双工模式

```
[SwitchA-Ethernet0/1]duplex full
```

（3）汇聚的端口速率要求相同，但不能是自适应

```
[SwitchA-Ethernet0/1]speed 100
```

（4）进入端口 E0/2

```
[SwitchA]interface Ethernet 0/2
```

（5）汇聚端口必须工作在全双工模式

```
[SwitchA-Ethernet0/2]duplex full
```

（6）汇聚的端口速率要求相同，但不能是自适应

```
[SwitchA-Ethernet0/2]speed 100
```

（7）根据源和目的 MAC 进行端口选择汇聚

```
[SwitchA]link-aggregation Ethernet 0/1 to Ethernet 0/2 both
```

三、SwitchB 交换机配置

```
[SwitchB]interface Ethernet 0/1
[SwitchB-Ethernet0/1]duplex full
[SwitchB-Ethernet0/1]speed 100
[SwitchB]interface Ethernet 0/2
[SwitchB-Ethernet0/2]duplex full
[SwitchB-Ethernet0/2]speed 100
[SwitchB]link-aggregation Ethernet 0/1 to Ethernet 0/2 both
```

实验 15　在同一个交换机上创建 VLAN

一、概述

本示例采用华为的 Quidway®S3026C-SIL2 线速以太网交换机。图 5.23 为在同一个交换机上创建 VLAN 的网络结构。SwitchA 端口 E0/1 属于 VLAN10，E0/2 属于 VLAN20。组网需求把交换机端口 E0/1 加入到 VLAN10，E0/2 加入到 VLAN20。

二、VLAN 的配置流程

（1）默认情况下所有端口都属于 VLAN1，并且端口是 access 端口，一个 access 端口只能属于一个 VLAN；

（2）如果端口是 access 端口，则把端口加入到另外一个 VLAN 的同时，系统自动把该端口从原来的 VLAN 中删除掉；

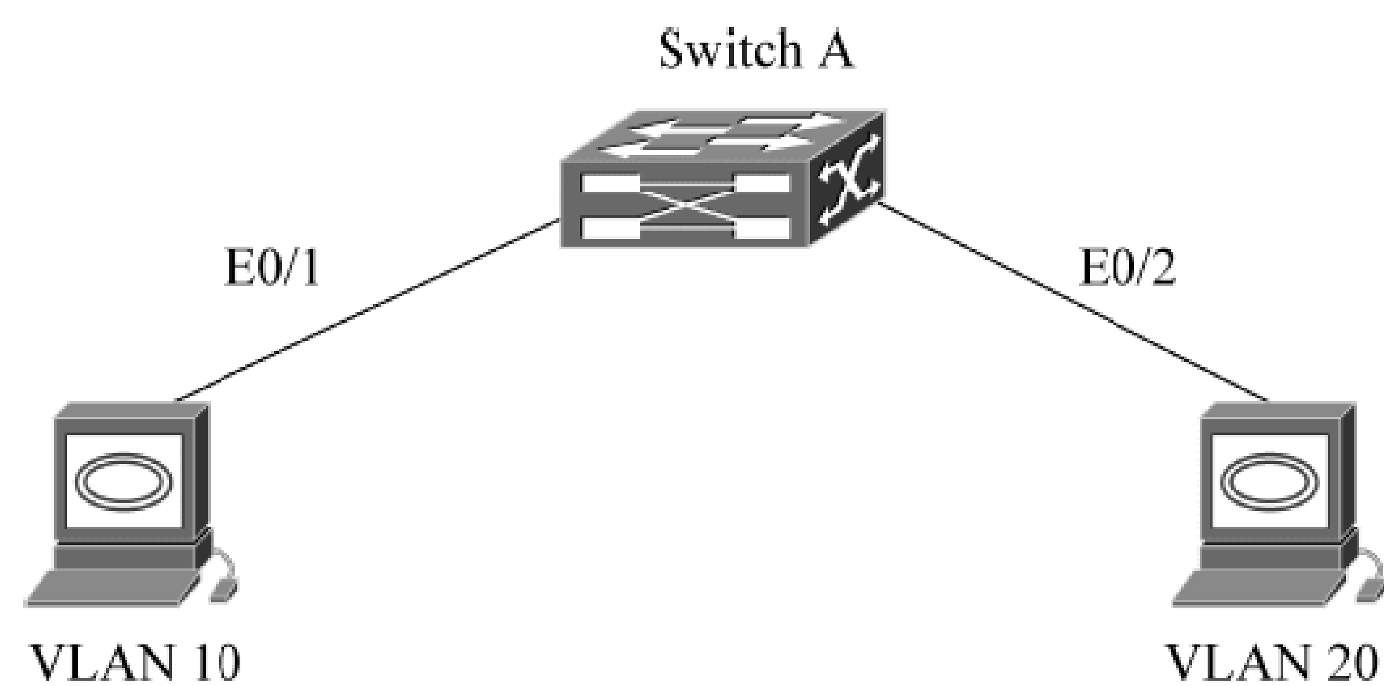


图 5.23　在同一个交换机上创建 VLAN 的网络结构

（3）除了 VLAN1，如果 VLAN XX 不存在，在系统视图下输入 VLAN XX，则创建 VLAN XX 并进入 VLAN 视图；如果 VLAN XX 已经存在，则进入 VLAN 视图。

三、说明

（1）请在用户视图（如<Quidway>）输入“system-view”（输入 sys 即可）进入系统视图。

（2）默认情况下，交换机端口为 access 端口，access 端口只属于 1 个 VLAN。

四、SwitchA 相关配置

创建（进入）vlan2：

```
[SwitchA]vlan 2
```

将端口 E0/1 加入到 vlan2：

```
[SwitchA-vlan2]port ethernet 0/1
```

创建（进入）vlan3：

```
[SwitchA-vlan2]vlan 3
```

将端口 E0/2 加入到 vlan3：

```
[SwitchA-vlan3]port ethernet 0/2
```

五、测试验证

（1）使用命令 disp cur 可以看到端口 E0/1 属于 vlan2，E0/2 属于 vlan3。

（2）使用 display interface Ethernet 0/1 可以看到端口为 access 端口，PVID 为 2。

（3）使用 display interface Ethernet 0/2 可以看到端口为 access 端口，PVID 为 3。

实验 16　在 Windows 下建立无线局域网

一、实验内容

在 Windows 7 下建立无线局域网。

二、实验准备

安装好无线网卡并装有 Windows 7 的计算机若干台。

三、实验参考步骤

主要实现以一台 Windows 7 为主机，在不同操作系统间建立无线局域网的方法。

1. *在主机上的设置*

（1）创建新的连接：控制面板→网络和共享中心→新建连接向导。

（2）选择无线临时网络，如图 5.24 所示。

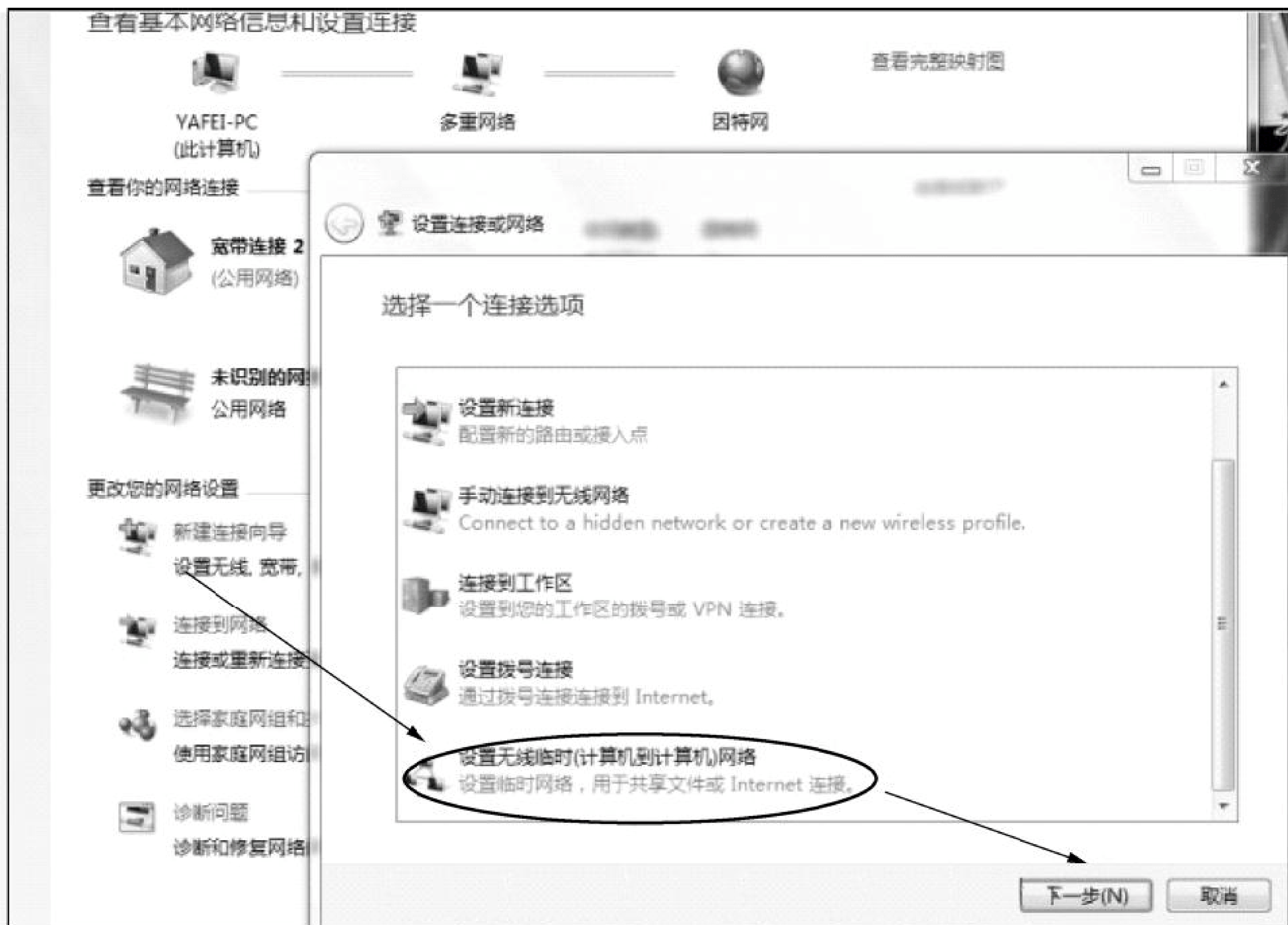


图 5.24　新建连接向导

（3）将安全类型设为无身份验证。

2. *设置 IP 及默认网关*

（1）要更改适配器设置，应右击无线网络连接，在弹出的快捷菜单中选择“属性”命令，选择“Internet 协议版本 4”选项，单击“属性”按钮，如图 5.25 所示。

（2）设置 IP 地址、子网掩码和默认网关。

IP 地址：192.168.0.1；子网掩码：255.255.255.0；默认网关：192.168.0.1，如图 5.26 所示。



图 5.25　打开无线网络属性

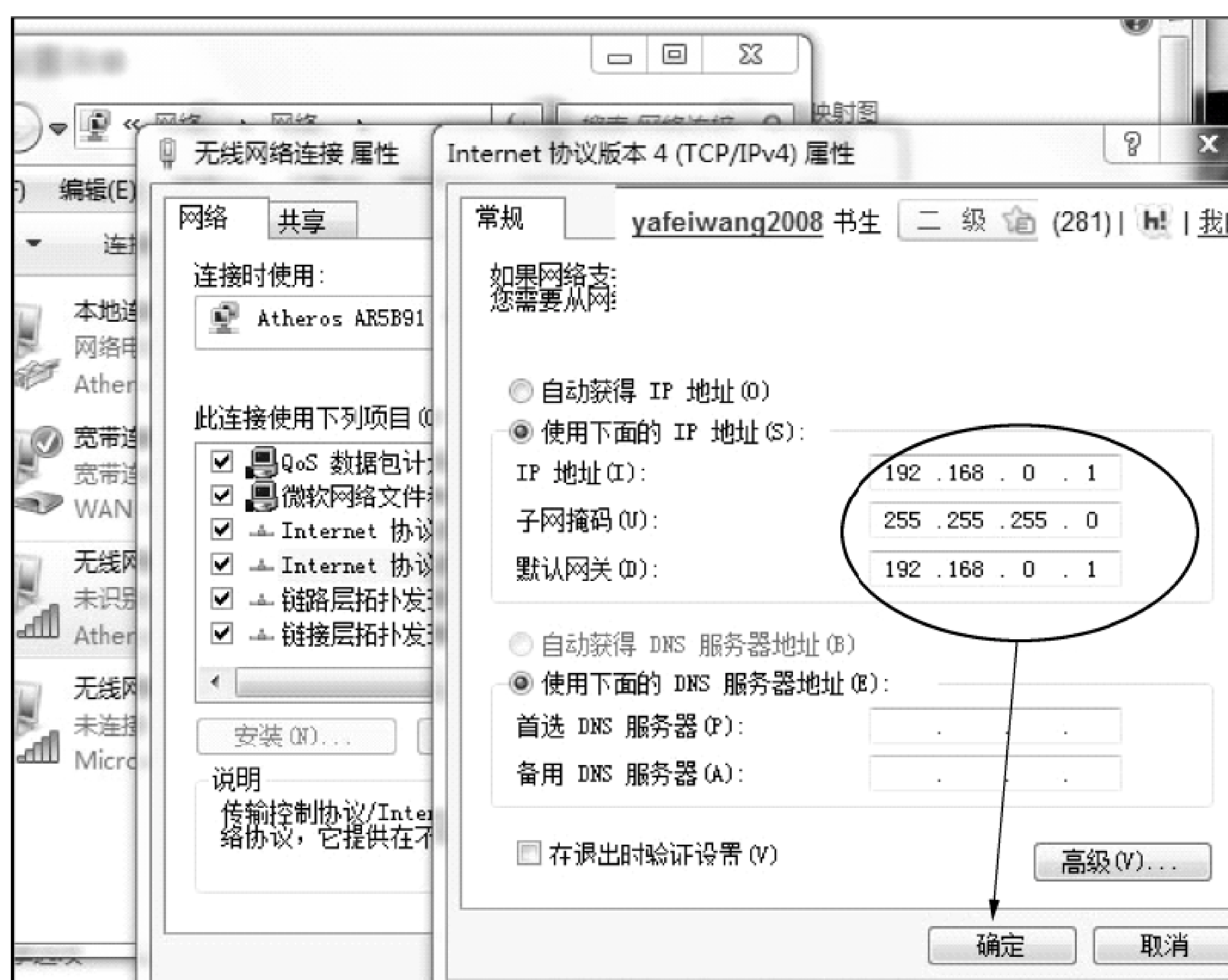


图 5.26　设置 IP 属性

（3）启用网络发现。启用网络发现，网络和共享→更改高级共享设置，如图 5.27 所示。
（4）关闭防火墙。在网络和共享里双击“Windows 防火墙”选项，如图 5.28 所示。

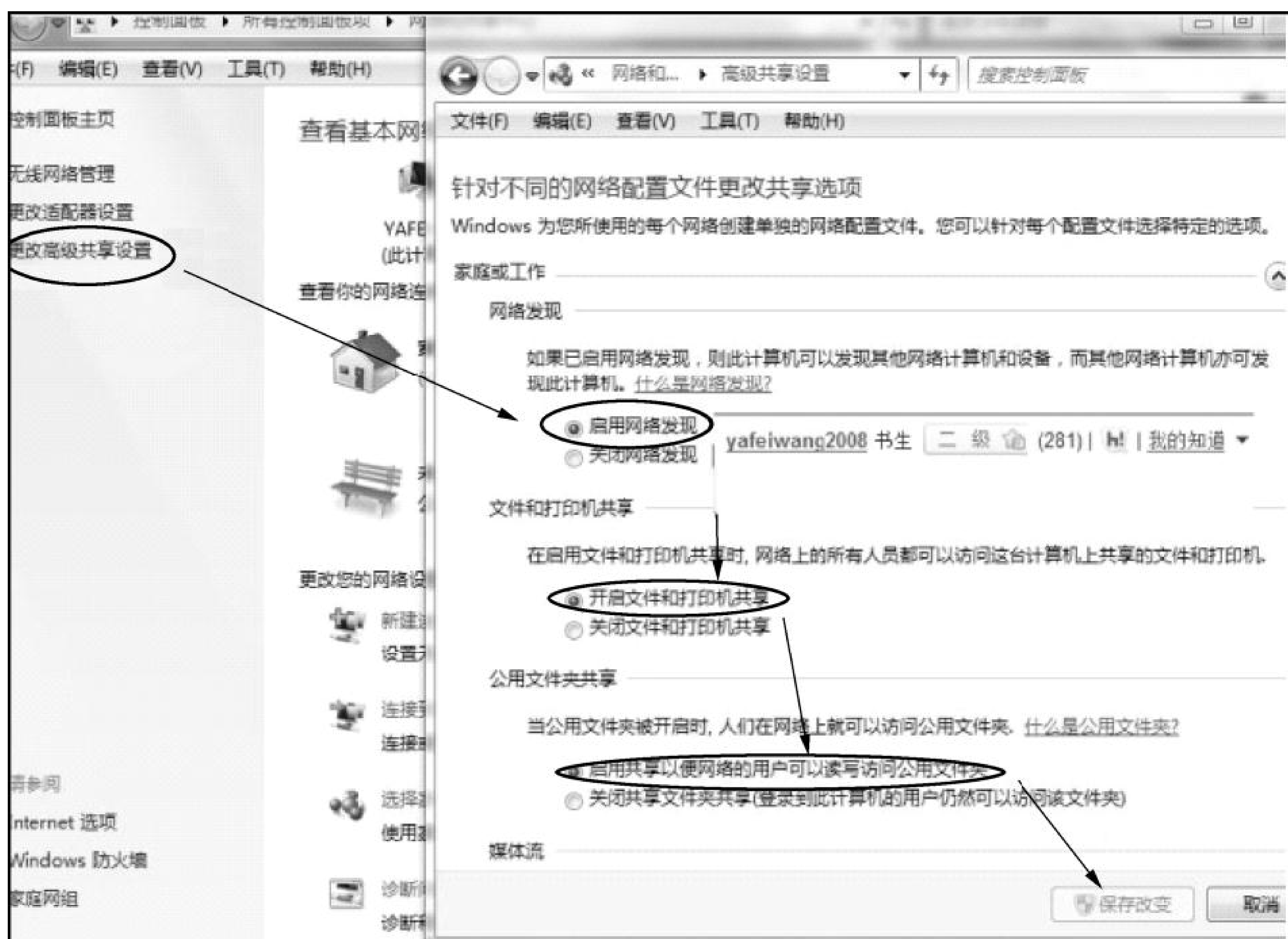


图 5.27　启用网络发现



图 5.28　打开 Windows 防火墙界面

关闭防火墙，如图 5.29 所示。

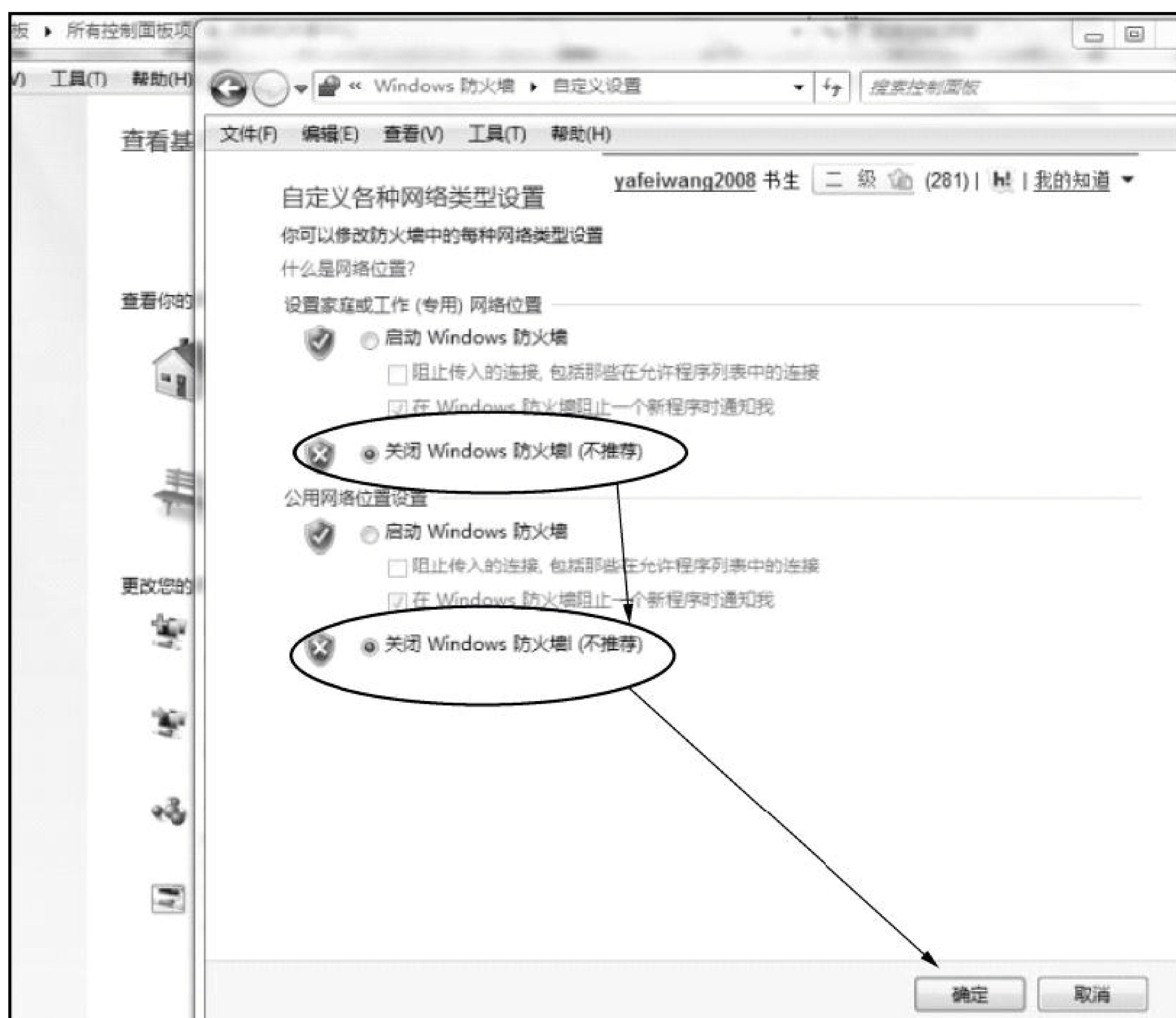


图 5.29　关闭防火墙

其他笔记本电脑的设置比较简单，只需重复上述步骤即可。设置完成后，搜寻主机刚建立的临时网络并连接即可。如果此时无法连接，可能是被 360 安全卫士或杀毒软件中的防火墙阻止了，注意将这些防火墙也关掉。

四、附加实验

Windows 7 与其他 Windows 系统在无线局域网中如何互相访问？

五、分析与讨论

为什么要关闭防火墙？

习　题　5

一、选择题

1．以下选项中，交换机会将帧发送到所有的端口中去的是【　　】。

A．交换机只知道接收帧的目的网卡的位置

B．交换机不知道接收数据包的目的网卡的位置

C．交换机不知道接收帧的目的网卡的位置

D．以上都不是

2．下列【　　】不是宽带路由器具有的功能。

A．集线器　　　　B．路由器　　　　C．NAT地址转换　　D．电话

3．目前，企业局域网一般选择【　　】网络拓扑结构。

A．总线型　　　　B．环形　　　　C．扩展星形　　　D．双总线型

4．下面【　　】是无线局域网的重要组成部分。

A．计算机主机　　B．以太网网卡　　C．无线AP　　　D．无线摄像头

5．100BASE-T Ethernet局域网中，下列说法不正确的是【　　】。

A．100指的是传输速率为100Mbps

B．BASE指的是基带传输

C．T指的是以太网

D．100BASE-T是Ethernet局域网的一种标准

6．下列关于局域网的叙述中，正确的叙述是【　　】。

A．地理分布范围大　　　　B．不包含OSI参考模型的所有层

C．误码率高　　　　　　　D．数据传输速率低

7．一座大楼内的一个计算机网络系统，属于【　　】。

A．网际网　　B．城域网　　C．局域网　　D．广域网

8．以下各项中，是CSMA/CD访问控制方法的标准是【　　】。

A．IEEE 802.3　　B．IEEE 802.4　　C．IEEE 802.6　　D．IEEE 802.5

9．以下选项不属于以太网的“5-4-3”原则的是【　　】。

A．5个网段　　　　　　　B．4个中继器

C．3个网段可挂接设备　　D．5个网段可挂接设备

二、填空题

1．局域网的参考模型中数据链路层又分为两个子层________和________。

2．在组建Windows对等网络的实验中，对等网络中的任意两台机器间要能够通信，共享网络资源，必须要在本地连接属性里添加的3个组件是：________、Microsoft网络用户和________。

3．10Mbps的以太网中，用集线器来扩展网络的范围时，最多只能级联________个集线器。

4．按拓扑结构分，局域网可分为________、________、________、树形拓扑结构。

三、简答题

1．CSMA有哪几种退让策略可以使用？各有什么特点？

2．查阅资料，比较10Mbps、100Mbps、1Gbps、10Gbps以太网层次结构和实现技术的异同。

3．为什么各种以太网都要定义多种物理层标准？

4．交换机有哪些分类方法？

5．VLAN的划分方法有哪几种？

6．蓝牙的主要技术特点是什么？

第 6 章　Internet 接入

将一个系统连接到另外一个系统，并获取服务，就称为接入。一台用户端计算机或局域网要访问 Internet 上的资源，首先要将计算机连接到 Internet 上。

6.1　Internet 接入概述

6.1.1　接入需求与接入类型

1．接入的基本要求

一般而言，用户对接入有如下一些基本要求：

（1）带宽要求。为了支持多媒体通信，要求较高的传输率，并且上、下行不对称，即对接收速率（即下行信道）的要求较高，对发送速率（上行信道）的要求较低。

（2）即连即用，即需要时就可以随时连通。

（3）价格便宜，工作可靠。

2．接入类型

目前，用户上网有多种方案可供选择，不同的 Internet 连接方式都是随着技术的不断发展以及不同的用户群需求而产生的。一般来说，个人（家庭）用户和企业用户的上网方式存在一定的区别。

1）按接入身份分类

按接入身份分类可分为仿真终端（作为某台主机的仿真终端，不分配 IP 地址）方式、主机方式和网络方式。

2）按接入方式分类

按接入方式即接入网的使用方式分类，可以分为直接接入和登录接入。直接接入是接入网的接入线永久地接在用户驻地网上，即用即通；登录接入指要先经登录，验证身份并在允许条件下才能连接。

3）按接入网络技术分类

按接入网络技术分类可分为 POST、HFC、ISDN、PLC、Wi-Fi、蓝牙、局域网等。不同的接入技术，使用不同的设备，如普通电话线接入需要使用 Modem。

4）按接入网介质分类

按接入网介质分类可分为铜线、光纤、光铜混合、无线、可见光等。有些接入技术是按介质设计的。如表 6.1 所示为接入网的类型。

表 6.1　接入网的类型

类　　型		系 统 类 别
有线接入	铜线传输	双绞铜线 线对增容系统（PG） 高比特数字用户线（HDSL） 非对称数字用户线（ADSL、VDSL、MDSL、XDSL 等）
	光纤传输	采用 Z 接口的用户环路载波系统（SLC） 采用 V5 国际标准接口的数字环路载波系统（V5-DLC） 采用 V5 国际标准接口的无光源网络（V5-PON） 模拟视频图像传输系统（VSB-AM，FM）
	光纤铜线混合	混合光纤/同轴传输系统（HFC） 交换式数字视像系统（SDV）
	电力线接入	
无线接入	固定终端	卫星直播系统（DHL） 同步卫星通信系统（SSC） 甚小孔径卫星终端（VSAT） 单区制无线接入 本地多点分布业务系统（LMDS） 多点多路分布业务系统（MMDS）
	移动终端	无线寻呼系统 无绳电话系统（CT1、CT2、DECT、PHS 等） 集群通信系统 蜂窝移动通信系统（TACS、AMDS、DAMPS、GSM、CDMA、DCS1800 等） 同步卫星移动通信系统（Inmarsat） 公共陆地移动通信系统（FPLMTS） 低轨道卫星移动通信系统（LEO） 蓝牙、Wi-Fi 等
有线无线综合接入	固定/移动终端	光纤无线混合系统（HFW） 个人通信系统（PCS） 可见光接入

5）按接入网频带分类

按接入网频带分类可以分为窄带和宽带。传统的接入网是窄带的，如电话网、ISDN、DDN 等。随着语音、视频、数据传输三网合一要求的日渐普遍，窄带将会很快退出历史舞台。因此，本章后面的各节以介绍宽带接入为主。

6）按 IP 地址分类

按是否需要 IP 地址可以分为如下几类。

（1）不需要 IP 地址：采用这种方式时，计算机作为远程主机的虚拟终端，只能享用电子邮件和 FTP 服务，不能使用 Web 等服务。

（2）使用动态地址接入：采用这种方式接入的计算机或网络（称 Intranet），可以访问 Internet 上的信息资源，但是由于没有固定的 IP 地址，Internet 上的其他用户不能访问该

Intranet 或计算机中的信息资源。这种方式收费较低，但需要向当地 ISP 申请一个联网账号。

（3）利用一个固定 IP 地址接入：这种接入方式允许 Intranet 访问 Internet 上的信息资源，也允许 Internet 访问 Intranet 上的信息资源。为了使用固定 IP 地址，Intranet 上的用户必须申请一个固定（静态）的 IP 地址。同时，由于共享 IP 地址会引起地址冲突，可以在 Intranet 中配置一个代理服务器。

（4）利用多个固定 IP 地址接入：对于大、中型 Intranet，利用一个固定 IP 地址接入时，随着 Intranet 与 Internet 之间信息交换频率的提高，将会出现“瓶颈”。此时，应当申请多个静态 IP 地址。

6.1.2 ISP

1. ISP 的服务

如图 6.1 所示，接入是通过 ISP 进行的。ISP 的狭义含义是 Internet service provider（Internet 服务提供商），广义的含义是 information service provider（信息服务提供商）。随着 Internet 的发展，二者的工作内容正在趋向相同。

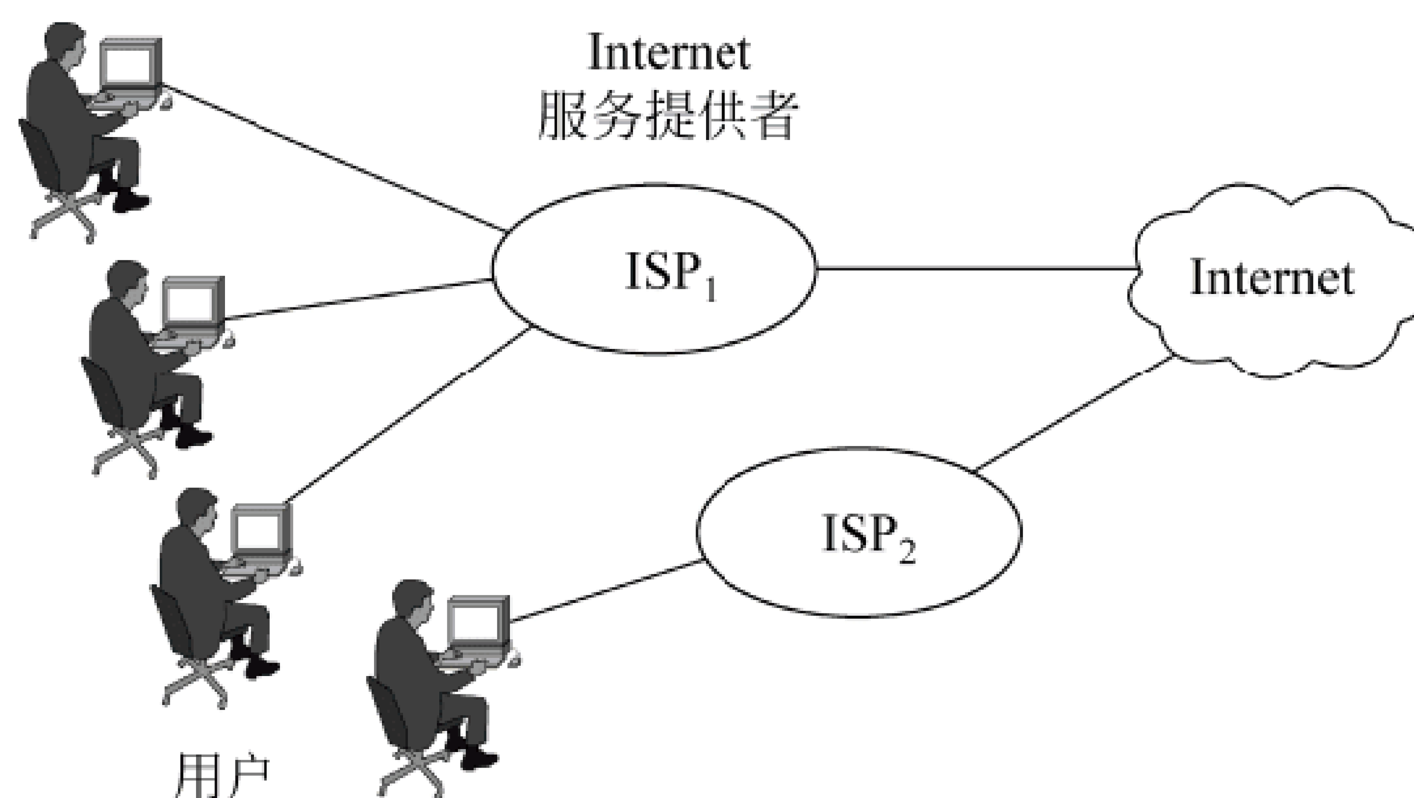


图 6.1 用户通过 ISP 接入 Interent

1）接入服务

ISP 为用户接入 Internet 提供设备（必要的服务器、路由器等）租用、高速通信线路用、地址分配、安装调试、系统管理（包括维护网络秩序，防止不文明行为对用户的侵扰等）服务。

2）系统集成

用户要接入 Internet，首先要配置计算机和网络通信系统，同时还要配置相应的系统软件以及 Internet 访问软件。这对没有专业力量的用户来说，就需要专门的公司帮助了。

对企业用户来说，在接入 Internet 或建设 Intranet 时，需要对企业进行认真调研，并根据企业的资金投入，综合分析网络的信息流量、结构、连接方式、费用等，着眼于全局进行入网方案的设计、规划、实施。所有这些服务，都可以从 ISP 那里得到。

3）信息服务

随着 Internet 应用的普及和深入，ISP 提供信息服务的比重将越来越大。目前，ISP 提供的信息服务有：提供信息共享和交流的服务设施，提供信息源和信息资源的增值开发。

提供信息共享和交流的服务设施的 ISP 也提供存储空间以及服务器的租用、代管，用

于存放共享和交流的各类信息，并承担这些信息资源的管理责任，如更新信息内容、为信息传递寻址、处理网络拥挤问题、尽量缩短用户的网络响应时间等。

信息资源的增值开发包括下列工作：查询检索服务（避免用户淹没在信息的海洋）、信息提取服务（代替用户访问网络）和信息分析服务（帮助用户分析研究，进行决策）。

还有一类 ISP，本身与计算机网络可以没有什么关系，但却可以通过 Internet 为用户提供信息查询和索引服务，如医院、图书馆、电子出版社、大学甚至政府等机构，通过向网上开放信息，为公众提供学习知识和有关信息。

4）Internet 应用

Internet 应用是指利用 Internet 开展业务活动，如学校利用 Internet 开展远程教学，企业利用 Internet 开展电子商务等。

2. ISP 的选择

一般说来，最终用户是通过 ISP 与 Internet 连接的。ISP 不仅要收取一定的费用，更重要的是，它的服务质量直接影响用户的上网质量。当前，ISP 日益增多，国内大型 ISP 有中国电信、中国移动、联通公司、广电公司等；小的 ISP 很多，以本单位或本地区的信息（网络）中心为主。面对众多的 ISP，用户一般可以从如下方面进行考虑。

1）收费标准

目前收费项目大致有开户费和使用费两大项。其中使用费又有许多计算方法，如按小时（又分白天、夜间、凌晨以及超时费等）、按月等。各家都有自己的收费方法和吸引用户的方法。用户应根据自己的使用特点，来确定哪一种收费方法对自己比较经济。

2）技术保证

用户最希望得到如下的技术保证：

- 拨号的成功率高，不希望想上网时多数碰上占线；
- 数据传输速率较高，不希望上网时一个文件传传停停，经常断线。

这些方面与 ISP 的下列技术条件有关：

- 有无先进可靠的设备，如交换机、路由器；
- 中继线数目，是否能满足众多的用户同时尤其是高峰期的拨入需求；
- 可以提供什么样的接入方式（仿真终端方式，还是 PPP 方式，或二者兼有之）；
- 出口速率，也即 ISP 与 Internet 连接的主干线的带宽；
- Modem 的标称速率，即 ISP 可以接收的用户 Modem 速率。当 ISP 可以接收的标称速率低于用户的实际 Modem 速率时，用户的 Modem 速率就不能发挥作用。

3）服务质量

ISP 能否提供上网的所有软件、资料，是否提供相应的技术培训等。

4）组织背景

经验历史、注册资本是否雄厚、财政是否稳定、经营状况、是否独立等。

关于 ISP 的情形，不仅要向 ISP 本身了解，还应当从它已有的用户等方面去了解、证实。

6.1.3 PPP 协议

1. PPP 协议及其特点

多数用户是通过 ISP 接入 Internet 的。PPP（Point-to-Point Protocol，点对点通信协议）为在点对点连接上传输多协议数据包提供了一个标准方法。它最初设计目的是为两个对等结点之间的 IP 流量传输提供一种封装协议以便通过拨号或专线方式建立点对点连接发送数据，使其成为各种主机、网桥和路由器之间简单连接的一种通用的解决方案。

具体地说，它具有如下特点：

（1）PPP 是一种用来同步调制连接的数据链路层协议——OSI 中的第二层。

（2）PPP 提供全双工操作，并按顺序传递数据包。

（3）PPP 具有动态分配 IP 地址的能力，允许在连接时刻协商 IP 地址。

（4）PPP 采用多协议成帧机制，不仅可以携带 IP 分组，还可以支持其他协议。

（5）PPP 具有错误检测以及纠错能力，支持选项协商、头部压缩以及使用 HDLC 类型帧格式(可选)的可靠传输。

（6）PPP 具有身份验证功能。

（7）PPP 可以用于多种类型的物理介质上，包括串口线、电话线、移动电话和光纤（例如 SDH）。

（8）PPP 简单，具有较高的互操作性。

2. PPP 帧格式

PPP 协议的一个核心工作是成帧：将每个 IP 分组可以毫无歧义地分割出一帧的起始和结束。PPP 的封装是精心设计的：

- 它可以封装多协议分组，并提供了不同网络层协议同时在同一链路传输的多路复用技术。
- 它能保持对大多数常用硬件的兼容性，使之成为一种多用途的点到点协议。
- 它不仅仅提供帧定界，而且提供协议标识和位级完整性检查服务。

如图 6.2 所示为将从 Internet 上接收到的数据 IP 分组封装成一个 PPP 帧。

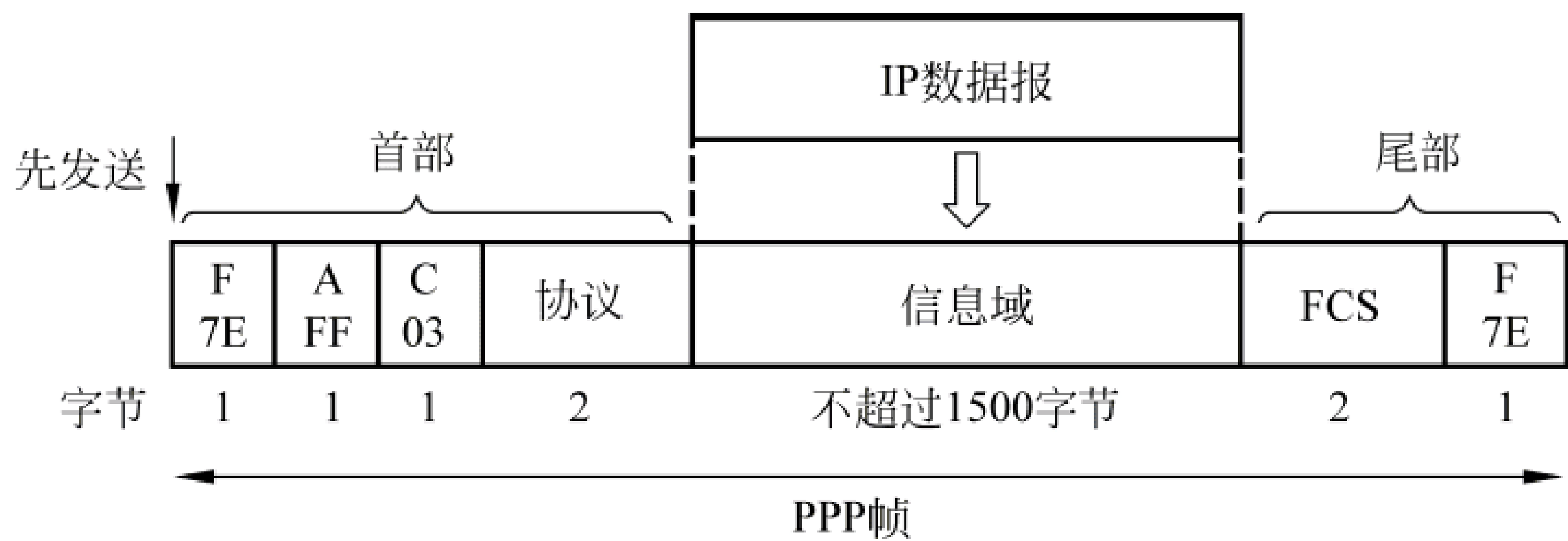


图 6.2　PPP 帧格式

其中：

（1）两个 F 字段是帧定界符——起始标志和结束标志，值为 01111110（0x7e）。因此所封装的信息可以不定长。如果在信息字段中出现 0x7e，为了不当成定界符，就要对该信息

字段进行填充：

在同步数据链路中，采用零比特填充法，即逢连续 5 个 1 就加 1 个 0；

在异步数据链路中，采用以 0x7d 为转义字符的字符填充法，同时要将第 6 个字符变反。例如，字符 0x7e→0x7d（01111101）+ 0x5e(01011110)，即将 0x7e——01111110 的第 6 位变反为 01011110——0x5e)，而字符 0x7d 要转换成 0x7d+0x5d（01111101 01011101）。

如果出现的连续的标志字段，就认为是空帧而被丢弃。

（2）A 是地址字段，值总是 0xff，表示这是一个广播地址，将该帧发向所有的站点。

（3）C 是控制字段，默认值为 0x03，表示无编号帧，即不提供使用帧编号和应答的可靠传输机制。

（4）协议字段指明信息字段中携带的数据的协议类型，使得 PPP 可以支持多种协议。图 6.3 为最常用的 3 种 PPP 协议帧中协议域与信息域部分。

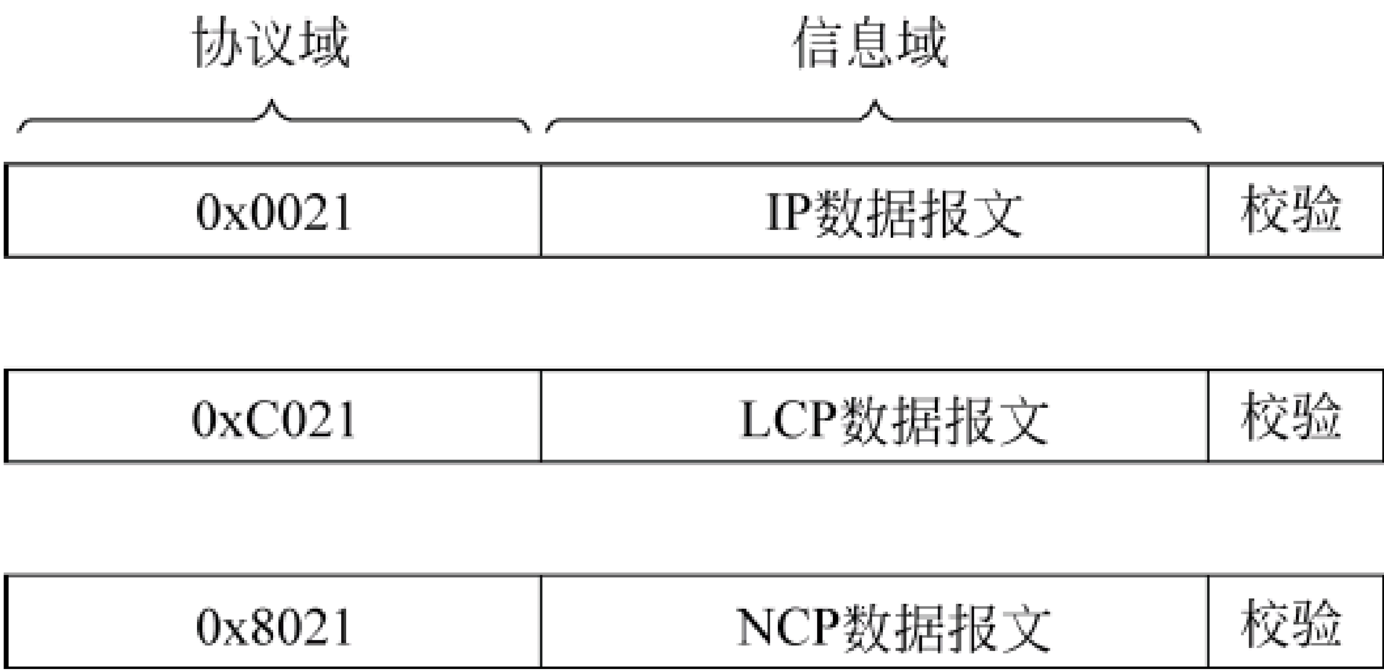


图 6.3　3 种常用 PPP 协议帧的协议域和信息域

协议字段的默认长度为 2 个字节，可以用 LCP 协商成 1 个字节。

（5）信息字段是被封装的数据，长度不超过 1500B。

（6）校验字段，使 PPP 协议在链路上具有差错检测功能。

3. PPP 协议栈

图 6.4 为 PPP 的协议栈结构。可以看到，PPP 是一个分层结构，它由建立在同步传输介质（如 ISDNH 或同步 DDN 专线）或异步传输介质（如基于 Modem 拨号的 PSTN 网络）的基础上的两层协议组成：下层是链路控制协议（Link Control Protocol，LCP），上层是网络控制协议族（Network Control Protocols，NCP）和 PPP 扩展协议族。

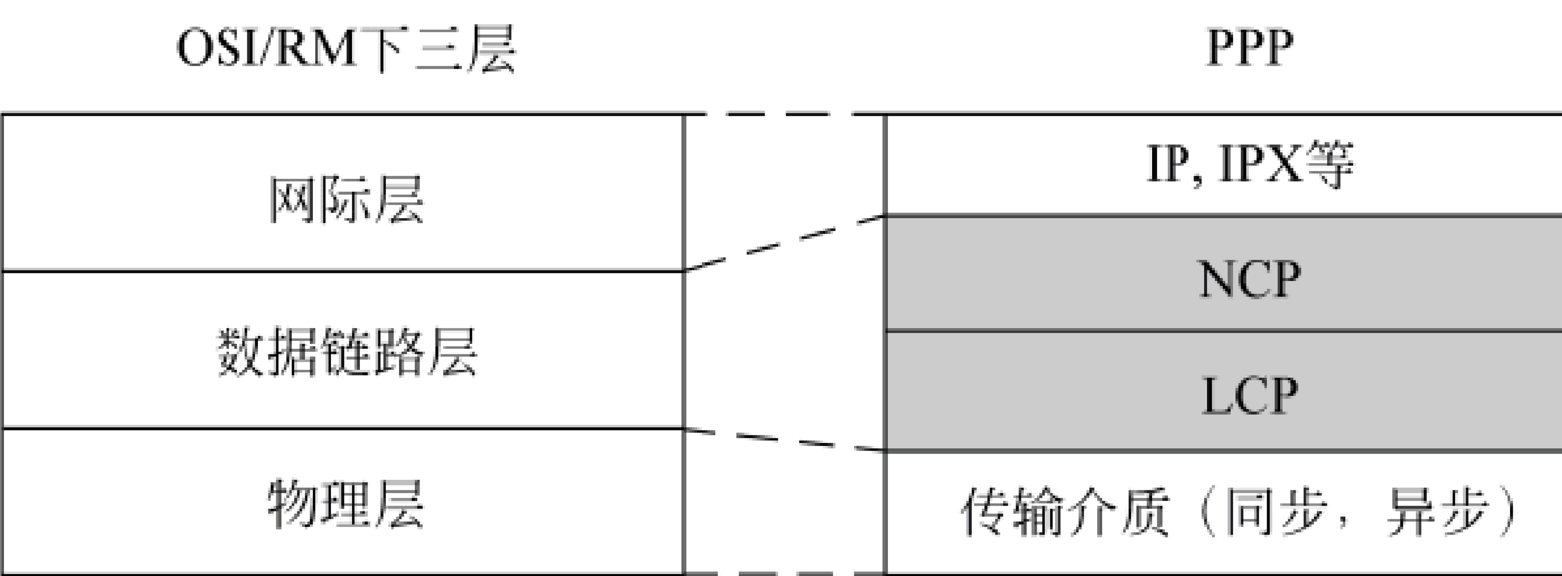


图 6.4　PPP 协议栈与 OSI/RM 下三层的对应关系

1）链路控制协议族（LCP）

LCP 是一种扩展链路控制协议位于物理层之上，是 PPP 中实际工作的部分，主要用于建立、拆除和监控 PPP 数据链路。它支持同步和异步线路，也支持面向字节的和面向位的

编码方式，可用于启动线路、测试线路、协商参数以及关闭线路。

2）网络控制协议族（NCP）

NCP 主要负责与上层的协议协商链路上所传输的数据包格式与类型，建立、配置不同的网络层协议。

3）PPP 认证协议

认证协议中最常用的包括口令验证协议（Password Authentication Protocol，PAP）和挑战-握手验证协议（Challenge-Handshake Authentication Protocol，CHAP）。

（1）PAP。PAP 有两个基本特点：明文验证方式和两次握手。其过程如图 6.5（a）所示分为两步：

① NAS（Network Access Server，网络接入服务器）要求用户提供用户名和口令；用户以明文方式回答用户名和密码。

② NAS 根据用户回答的正确与否，决定发 ACK（验证成功，允许进入下一阶段）或 NAK（验证失败）。验证失败并不会直接将链路关闭。只有当验证不通过次数达到一定值（默认为 4）时，才会关闭链路。

很明显，这种验证方式的安全性较差，第三方可以很容易地获取被传送的用户名和口令，并利用这些信息与 NAS 建立连接获取 NAS 提供的所有资源。所以，一旦用户密码被第三方窃取，PAP 就无法提供避免受到第三方攻击的保障措施。

（2）挑战-握手验证协议（CHAP）。CHAP 有如下 3 个基本特点。

- 挑战方式：验证方（NAS）首先发起验证请求（也就是挑战信息）——挑战口令（challenge）。
- 加密验证：挑战口令。
- 是一个 3 次握手过程。如图 6.5（b）所示，3 个步骤为：

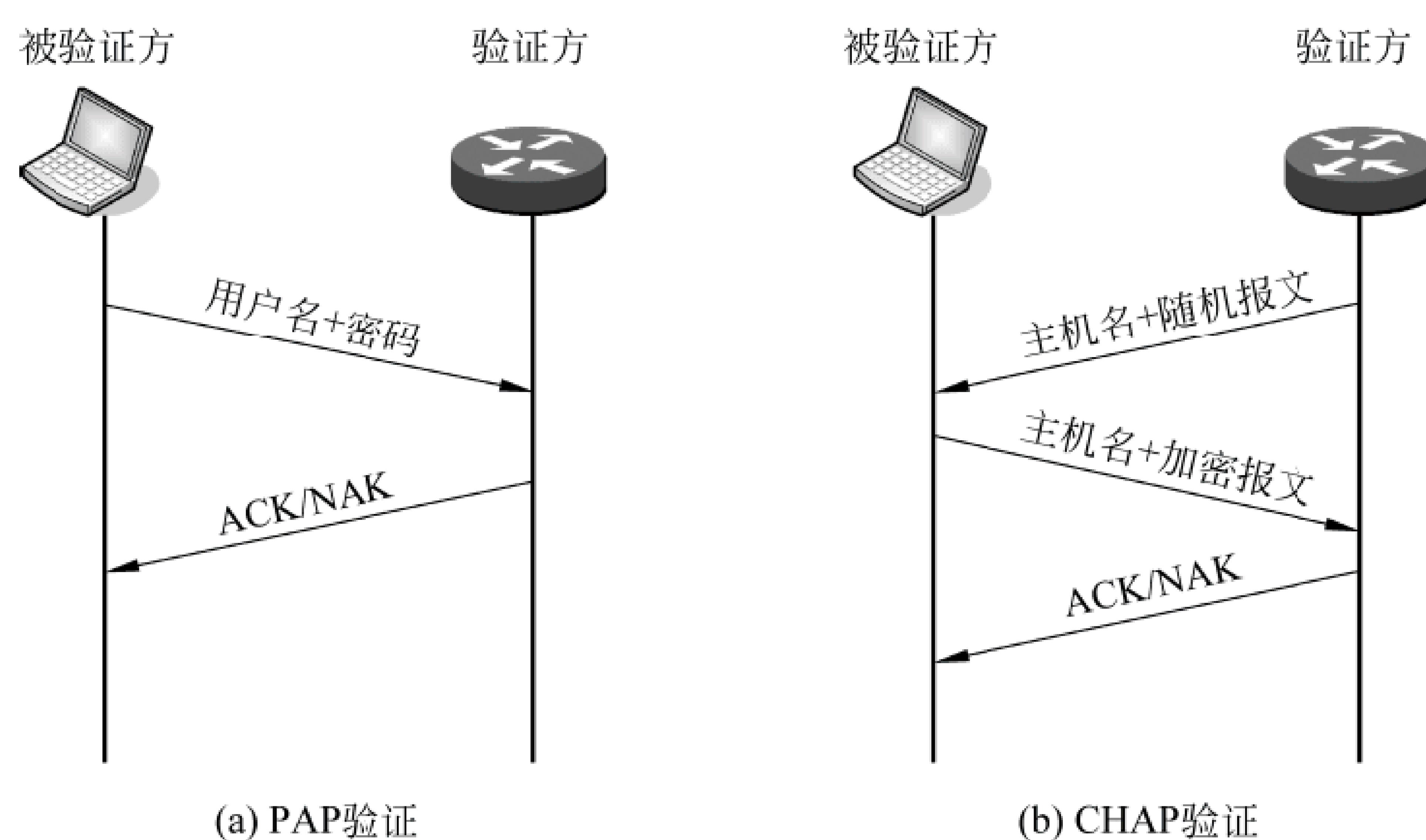


图 6.5　PAP 验证和 CHAP 验证过程

① 验证方向被验证方发送一个验证请求（Challenge）报文，内容是一个会话 ID 和一个随机产生的挑战字串（arbitrary challengestring），并附带上本端的主机名。

② 被验证方接到对端对本端的验证请求时，要返回一个应答（response）报文。报文中包含着用 MD5 单向哈希算法（one-way hashing algorithm）生成加密的挑战字串、会话

ID、用户口令和非哈希方式的自己的用户名。这里，可将 MD5 算法看作为一种特别的加密算法。

③ 验证方接到此应答后，利用对端的用户名在本端的用户表中查找本方保留的口令字，用本方保留的口令字（密钥）和随机报文用 MD5 算法得出结果，与被验证方应答比较，根据比较结果返回相应的结果（ACK 或 NAK）。

这种方式能够避免建立连接时传送用户的真实密码，因此它的安全性要比 PAP 高。

4）IPCP

IPCP（IP Control Protocol，IP 控制协议）负责建立，使用和中止 IP 模块。IPCP 和 LCP 协议使用相同的包交换机制。IPCP 包在 PPP 没有达到网络层协议阶段以前不能进行交换，如果有 IPCP 包在到达此阶段前到达会被抛弃。

4. PPP 工作过程

图 6.6 描述了 PPP 的工作状态变化和工作过程。这些状态包括了链路静止（link dead）、链路建立（link establish）、鉴别（authenticate）、网络层协议（network-layer protocol）协商、链路开启（link open）和链路终止（link terminate）。这些状态变化也将 PPP 的工作过程分为相应的阶段。

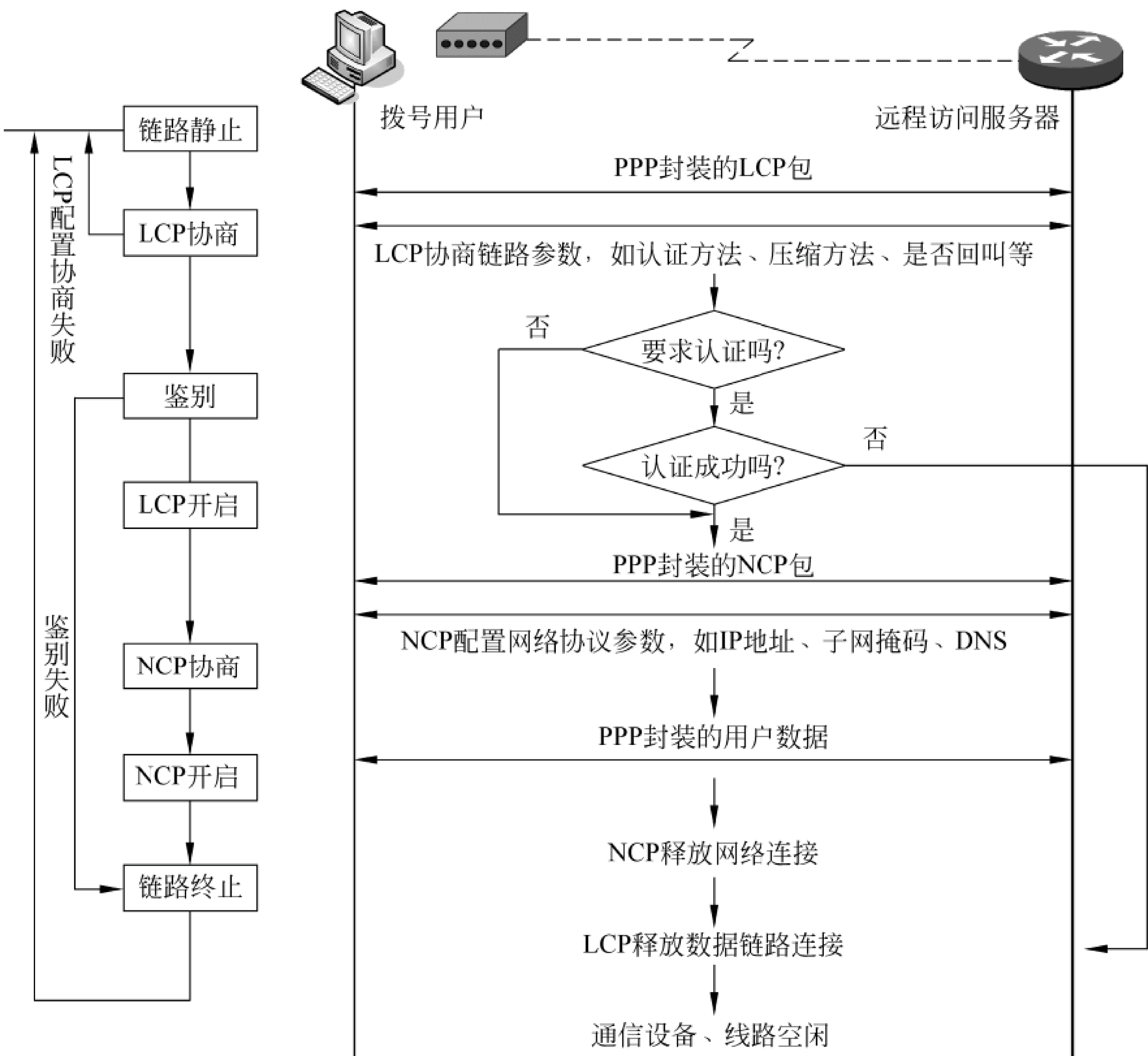


图 6.6　PPP 工作过程

PPP 的核心工作是配置，这些配置是通过协商进行的，在不同阶段按不同协议进行协商；并且只有前面的协商出现结果后才能转到下一个阶段，进行下一个协议的协商。

1）链路静止阶段

当物理层不可用时，PPP 链路处于“静止”（dead）阶段。链路必须从这个阶段开始和结束。

2）LCP 协商阶段

当用户通过 MODEM 呼叫（通常是用鼠标点击一个连接图标）接入路由器时，路由器就能检测到 MODEM 发出的载波信号，物理连接就可以建立。这时，PPP 进入 LCP 协商状态——目的是建立 LCP 连接，对基本的通信方式进行协商选择，内容包括：工作方式是 SP（Single-link PPP，单 PPP 通信）还是 MP（Multilink PPP，多 PPP 通信，允许将报文分片，提供多条 PPP 链路捆绑发送到统一目的地）、鉴别协议的规约、最大传输单元等配置选项。

这个过程通过链路连接的两端通过 LCP 向对方发送配置信息报文（configure packets）完成。表 6.2 为 4 种最常用 LCP 报文种类及其作用。

表 6.2　4 种最常用 LCP 报文种类及其作用

编码字段值	LCP 帧类型	说　明
1	LCP 配置请求帧（configure-request）	在打开或重置 PPP 连接时，修改默认 LCP 选项
2	LCP 配置确认帧（configure-ACK）	所有选项都接受
3	LCP 配置否认帧（configure-NAK）	所有选项都理解，但不能接受
4	LCP 配置拒绝帧（configure-reject）	有的选项无法识别或不能接受，需要再协商

LCP 协商过后，LCP 变为“开启”状态，表示链路已经建立。

3）鉴别阶段

鉴别协议需要手工配置。如果配置了鉴别协议，就进入鉴别阶段，开始 CHAP 或 PAP 鉴别。如果验证失败进入终止状态，拆除链路，LCP 状态转为“下线”（down）；如果验证成功，就进入网络阶段，由 NCP 协商网络层参数。此时，LCP 状态仍为“开启”，而 IPCP 状态从“初始”转到“请求”（request），进入网络协议阶段。

4）NCP 阶段

NCP 协商支持 IPCP 协商。IPCP 协商主要包括双方的 IP 地址，通过 NCP 协商来选择和配置一个网络层协议。当选中的网络层协议配置成功后，该网络层协议就可以通过这条链路发送报文了。此后，PPP 链路将一直保持通信。直至有明确的 LCP 或 NCP 帧关闭这条链路，或发生了某些外部事件（例如用户的干预）。

5）链路终止阶段

链路终止阶段会在两种情况下进入：

（1）数据传送结束，一方发出 LCP 请求终止帧，另一方发出终止确认帧后。

（2）链路出现故障。

之后，Modem 关闭，载波停止，回到“静止”状态。

6.1.4 PPPoE 协议

随着宽带以太网的发展和广泛应用，基于以太网的 PPP（PPP over Ethernet，PPPoE）于 1998 年应运而生。

1. PPPoE 的技术特点

在采用总线或集线器连接网络中，每一台主机可能需要连接的 AC（Access Concentration，接入集中器也可以看作是接入交换机）是不相同的。因此，为了维护一台主机与 AC 之间的点到点关系，每台主机与自己的那个 AC 之间能建立唯一的点到点会话，即所有的主机都需要能够独立地配置自己的 PPP 协议栈。为此，PPPoE 工作分为两个阶段：PPPoE 的发现阶段（PPPoE Discovery Stage）和 PPPoE 的会话阶段（PPPoE Session Stage）。

当一个主机想开始一个 PPPoE 会话时，首先会以广播式到网络上寻找所有的 AC，然后从中选择一个，并获取其以太网 MAC 地址。在这个过程中，AC 会为每一个 PPPoE 会话分配一个唯一的 PPPoE 会话标识号（PPPoE session-ID）。

会话建立起来后才可以开始 PPPoE 的会话阶段。

2. PPPoEz 帧与数据报文格式

1）PPPoE 帧格式

PPPoE 可以理解为在以太网上跑 PPPoE 帧。因此，其帧格式与以太网帧格式一致，如图 6.7 所示。

<table>
<tr><td colspan="2">目标MAC地址
(6B)</td><td colspan="2">源MAC地址
(6B)</td><td>以太类型
(2B)</td></tr>
<tr><td colspan="3">载荷
(46~1500B)</td><td colspan="2">校验码
(4B)</td></tr>
</table>

图 6.7 PPPoE 帧格式

其中：

目的地址和源地址：都是 6B，即 MAC 地址。

类型：用于区分承载的数据报文用于哪个阶段。

- 发现阶段的帧：0x8863。
- 会话阶段的帧：0x8864。

2）数据报文格式

会话报文格式如图 6.8 所示。

<table>
<tr><td>版本
(0x1)</td><td>类型
(0x1)</td><td>代码
(1B)</td><td>会话-ID
(2B)</td><td>长度
(2B)</td></tr>
<tr><td colspan="5">净负荷</td></tr>
</table>

图 6.8 PPPoE 数据报文封装格式

其中：

- 版本域，占 4b，协议中明确的规定，这个域的内容填充 0x01。

- 类型域，占 4b，协议中同样规定，这个域的内容填充为 0x01。
- 代码域，占 1B，对于 PPPoE 的不同阶段这个域内的内容也不一样。
- 会话 ID，占 2B，当访问集中器还未分配唯一的会话 ID 给用户主机时，则该域内的内容必须填充为 0x0000，一旦主机获取了会话 ID 后，那么在后续的所有报文中该域必须填充那个唯一的会话 ID 值。
- 长度域，占 2B，用来指示 PPPoE 数据报文中净载荷的长度。
- 净负荷域，即数据域。在 PPPoE 的不同阶段，该域内的数据内容会有很大的不同。在 PPPoE 的发现阶段时，该域内会填充一些 Tag（标记）；而在 PPPoE 的会话阶段，该域则携带的是 PPP 的报文。

3）Tag（标记）格式

发现阶段的 PPPoE 数据报文中，净载荷可能包含零个或多个 Tag（标记）。这些标记也是要经过协商。承载在 PPPoE 报文数据域中的标记封装格式如图 6.9 所示。

Tag类型 (2B)	Tag长度 (2B)	Tag 数据

图 6.9　PPPoE 数据报文中标记的封装格式

其中：

- 标记长度域为 2B，用来指明标记数据域的长度。
- 标记的数据域中用来放置不同类型标记所对应的相关数据。
- 标记类型于为 2B。表 6.3 列出了各种标记类型的含义。

表 6.3　各种标记类型的含义

标记类型	标 记 说 明
0x0000	表示 PPPoE 报文数据域中一串标记的结束，为了保证版本的兼容性而保留，在有些报文中有应用
0x0101	服务名，主要用来表明网络侧所能提供给用户的一些服务
0x0102	访问集中器名，当用户侧接收到了 AC 的回应的 PADO 报文时，就可获从所携带的标记中获知访问集中器的名字，而且还可以据此来选择相应的访问集中器
0x0103	主机唯一标识，类似于 PPP 数据报文中的标识域，主要是用来匹配发送和接收端的，因为对于广播式的网络中会同时存在很多个 PPPoE 的数据报文
0x0104	AC-Cookies，主要被用来防止恶意性 DOS 攻击
0x0105	销售商的标识符
0x0110	中继会话 ID，对于 PPPoE 的数据报文也同样可以像 DHCP 报文一样被中断到另外的 AC 上终结，这个字段则是用来维护另一个连接的
0x0201	服务名错误，当请求的服务名不被对端所接受时，会在响应的报文中携带这个标记
0x0202	访问集中器名出错
0x0203	一般性错误

3. PPPoE 工作过程

如图 6.10 所示，PPPoE 的工作可以分为 3 个阶段。

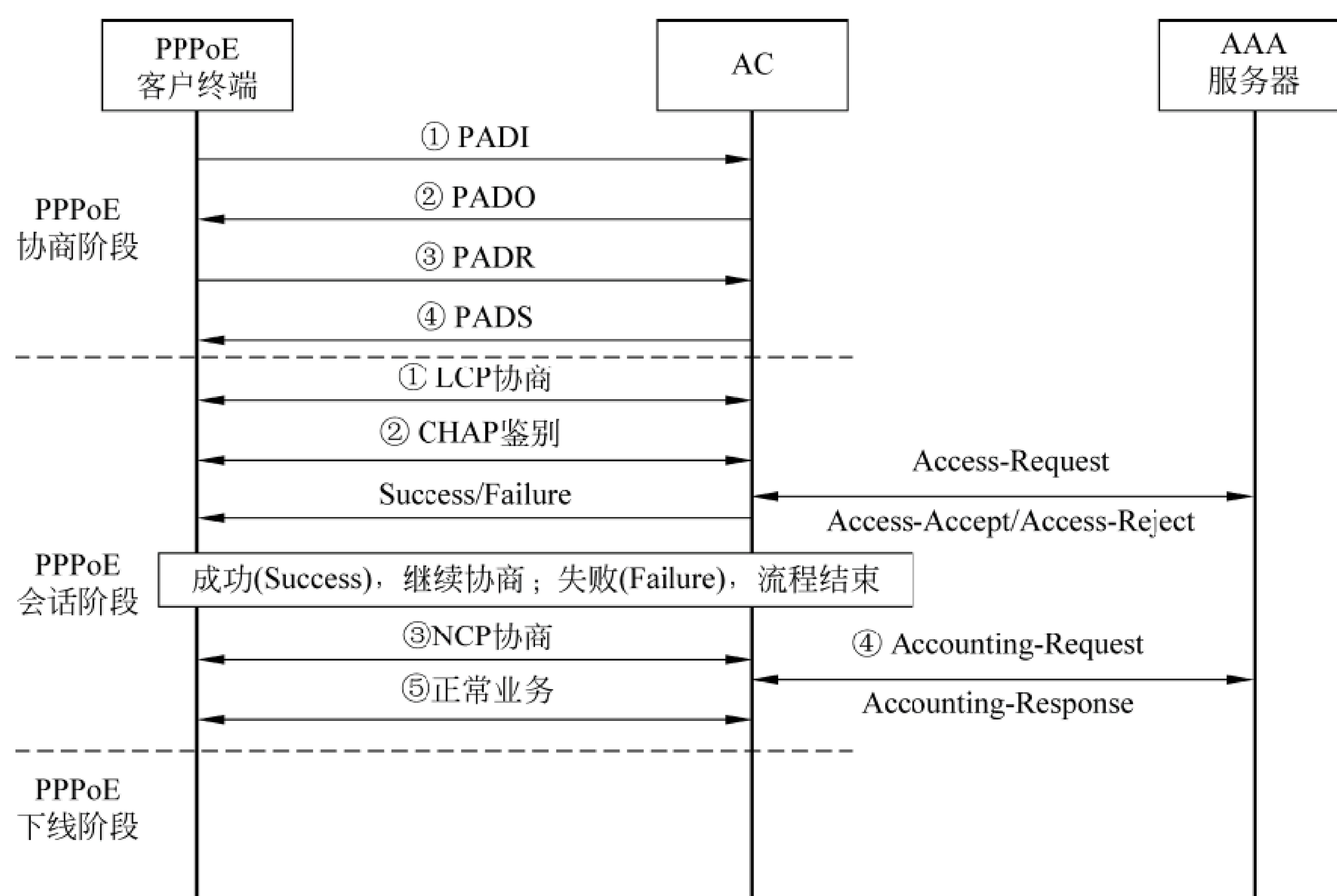


图 6.10　PPPoE 的工作过程

1）PPPoE 的发现阶段

在发现（Discovery）阶段中，结点之间处于无连接的客户端-服务器关系直到一个 PPPoE 会话建立。这个阶段分 4 步完成。

（1）主机发广播帧寻找 AC 或交换机。发起分组 PADI（PPPOE Active Discovery Initiation）中含有下列内容。

- 目的地址：0xffffffffffff——以太网的广播地址。
- CODE（代码）字段值为 0x09。
- SESSION-ID（会话 ID）字段值为 0x0000。
- 至少包含一个服务名称类型的标签（标签类型字段值为 0x0101），提出服务要求。

（2）符合服务范围的 AC 收到 PADI 分组后，发送 PPPoE 有效发现提供包 PADO（PPPoE Active Discovery Offer）分组，响应请求。其中包含：

- CODE 字段值为 0x07。
- SESSION-ID 字段值仍为 0x0000。
- AC 的 MAC 地址。
- 一个含 AC 名称类型的标签（标签类型字段值为 0x0102）。
- 必须包含一个或多个服务名称类型标签，表明可向主机提供的服务种类。

（3）主机在收到的多个 PADO 分组中选择合适的一个，然后向所选择的 AC 发送 PPPoE 有效发现请求分组 PADR（PPPoE Active Discovery Request）。其中包含：

- CODE 字段为 0x19。
- SESSION_ID 字段值仍为 0x0000。
- 必须包含一个服务名称类型标签，确定向接入集线器（或交换机）请求的服务种类。

若主机在指定的时间内没有接收到 PADO，它应该重新发送它的 PADI 分组，并且将等待时间加倍，这个过程会被重复期望的次数。

（4）AC 收到 PADR 分组后准备开始 PPP 会话，它发送一个 PPPoE 有效发现会话确认 PADS（PPPoE Active Discovery Session-confirmation）分组。其中包含：

- CODE 字段值为 0x65。
- SESSION-ID 字段值为接入集中器所产生的一个唯一的 PPPoE 会话标识号码。
- 必须包含一个接入集中器名称类型的标签以确认向主机提供的服务。

当主机收到 PADS 分组确认后，双方就进入 PPP 会话阶段。这时，用户主机和接入设备都必须为 PPP 虚拟端口分配资源。

2）PPPoE 的会话阶段

PPPoE 的会话阶段分为 5 个子阶段：LCP 协商、CHAP 鉴别、开始计费、NCP 协商和报文传输。

（1）客户端与 AC 之间进行 PPP 的 LCP 协商，同时使用 CHAP 认证。

（2）LCP 协商的同时进行 CHAP 鉴别：

- AC 向客户端发送一个含有挑战字串等信息的 Challenge 报文。
- 客户端收到 Challenge 报文后，对密码和 Challenge 执行 MD5 算法后的，在 Response 回应报文中把它发送给 AC。
- AC 将 Challenge、Challenge-Password 和用户名一起送到 RADIUS 用户认证服务器，由 RADIUS 用户认证服务器进行认证。
- RADIUS 用户认证服务器根据用户信息判断用户是否合法，然后回应认证成功/失败报文到 AC。如果成功，携带协商参数以及用户的相关业务属性给用户授权。如果认证失败，则流程到此结束。
- AC 认证结果返回给客户端。

（3）用户进行 NCP（如 IPCP）协商，通过 AC 获取到规划的 IP 地址等参数。

（4）认证成功，启动计费程序。

- AC 向 RADIUS 用户认证服务器发起计费开始请求。
- RADIUS 用户认证服务器对计费开始请求响应。

（5）用户获得合法权限，可以开始正常的网络业务。

一旦 PPPoE 进入到会话阶段，则 PPP 的数据报文就会被填充在 PPPoE 的净载荷中被传送，这时两者所发送的所有以太网包均是单目地址。PPPoE 会话阶段以太网帧的协议域填充为 0x8864，代码域填充 0x00，整个会话的过程就是 PPP 的会话过程，但在 PPPoE 数据域内的 PPP 数据帧是从协议域开始的。此外，PPPoE 会话的 SESSION-ID 一定不能改变，并且必须是发现阶段分配的值。

3）PPPoE 下线流程

PPPoE 用户下线流程包括用户主动下线和异常下线两种情况。

（1）用户主动下线流程如下：

① 用户通过 PPPoE 客户端，主动向 AC 发送 Terminate-Request。

② AC 向 PPPoE 客户端返回 Terminate-Ack 报文。

③ PPPoE 服务器向 AAA 服务器发送计费停止请求的报文。

④ AAA 服务器向认证点回计费停止请求报文的回应。

（2）异常下线流程如下：

① AC 检测到用户已经不在线。

② AC 向 AAA 服务器发送计费停止请求的报文。

③ AAA 服务器向认证点回计费停止请求报文的回应。

在 PPP 架构中，用户通常会通过传送 IPCP（IP 控制协议）终止消息而中断已建立的会话。否则，LCP（链路控制协议）周期性轮检机制能够检测出 PPP 会话是否已终止。如果检测到会话已中止，则分配给用户终端的 IP 地址将被释放回 IP 地址池中。因此，由于 PPP 会话的安全性、健壮性等特征，而被广泛应用于 ADSL 接入认证。

（3）PPPoE 还有一个 PADT 分组，它可以在会话建立后的任何时候发送，来终止 PPPoE 会话，也就是会话释放。它可以由主机或者 AC 发送。当对方接收到一个 PADT 分组，就不再允许使用这个会话来发送 PPP 业务。PADT 分组不需要任何标签，其 CODE 字段值为 0xa7，SESSION-ID 字段值为需要终止的 PPP 会话的会话标识号码。在发送或接收 PADT 后，即使是正常的 PPP 终止分组也不必发送。PPP 对端应该使用 PPP 协议自身来终止 PPPoE 会话，但是当 PPP 不能使用时，可以使用 PADT。

6.2 铜 线 接 入

6.2.1 综合业务数字网

综合业务数字网（Integrated Services Digital Network，ISDN）兼有 IDN（综合数字电话网）和 ISN（综合业务网）两重含义。ISDN 的工作原理如图 6.11 所示，它能将数据、声音、视频信号集成进一根数字电话线路，实现用户线传输技术数字化，向用户提供端到端的数字连接，所以被称为“一线通”。

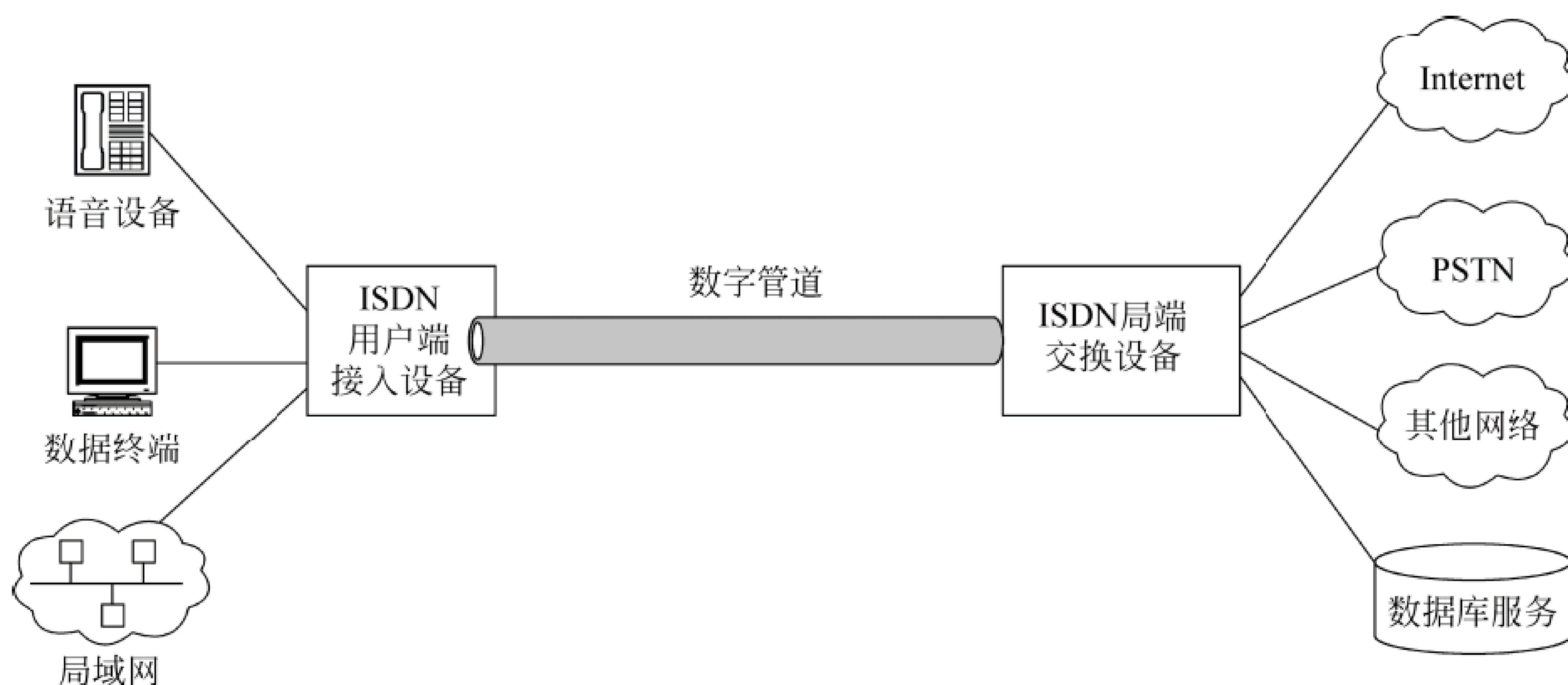


图 6.11　ISDN 工作原理

1. ISDN 的信道与接口

ISDN 采用 TDM 技术，将多条通路复用在 ISDN 的数字管道中，依时段分配给各信号源，并提供多种独立的信道供用户使用。这些信道采用 ITU-T 规定的标准信道系列。

1）ITU-T 标准信道系列

ITU-T 标准信道系列用字母来称呼：

A 信道——3kHz 带宽的标准模拟话路信道；

B 信道——63kbps 的数字 PCM 话音或数据信道；

C 信道——8/16kbps 的数字信道；

D 信道——用作通信控制（带外信令）的数字信道；D0 为 16kbps，D2 为 63kbps；

E 信道——63kbps 内部 ISDN 信令的数字信道；

H 信道——高速接入通路，适合于电视会议、超图像传输、高速 FAX、高速数据等信息的传送。目前 H 通路具有如下 3 种标准速率。

- H_0 通路：383kbps，用于传送用户信息。
- H_{11} 通路：1 536kbps（PCM23 路系统），用于传送用户信息。
- H_{12} 通路：1 920kbps（PCM32 路系统），用于传送用户信息。

2）ITU-T 标准化信道组合

ITU-T 规定了多种标准化信道组合，其中最重要的是基本速率接口（Base Rate Interface，BRI）和基群速率接口（Primary Rate Interface，PRI）。

（1）基本速率接口是为普通电话网的用户提供的一种窄带服务，具有 2B+D 接口。其中：

- 2 个 B 通路为 63kbps，用于传输话音；
- D 通路为 16kbps 或 63kbps，用于传送信令信息和分组信息。

（2）基群速率接口是指适应 PCM 一次群 T1（1.533Mbps）或 E1（2.038Mbps）的通路，给出了多个基本访问用户通过一个公用线路设施与网络相连的规则，提供宽带服务（称 B-ISDN），组合形式如下。

- 多信道接入（B 信道接口）：nB+D，n=30（欧洲、澳洲等，总带宽达 2.038Mbps）或 23（美国、日本等，总带宽达 1.533Mbps）。
- 高速接入（H 信道接口）：典型结构有 mH_0+D（m=3 或 5）、H_{11}+D、H_{12}+D 等。
- 组合接入（B/H 信道混合接口）：nB+mH_0+D（$n+6\times m\leqslant 30$ 或 23）。

B-ISDN 采用了 ATM 技术。由于 ATM 技术没有得到广泛应用，B-ISDN 使用也很少。

2. ISDN 接入设备

ISDN 按照自己的规格将设备分为两类：ISDN 标准设备和非 ISDN 标准设备。ISDN 标准设备（如数字电话等）可以使用网络终端（Network Terminal，NT）接入；非 ISDN 标准设备（如普通电话、传真机、计算机等）还要在 NT 上增加使用 ISDN 终端适配器（Terminal Adapter，TA）。如图 6.12 所示为上述两种接入的示意图。

1）网络终端（NT）

NT 安装于用户处，用于实现在普通电话线上进行数字信号的转送和接收，是电话局程控交换机和用户终端设备之间的接口设备。NT 分为两种：NT1 和 NT2。

NT1 是基本速率接口终端，向用户提供 2B+D 的两线双向传输能力，它是物理层的设备，不涉及比特流在上层是怎样构成帧的，它能以点对点的方式最多支持 8 个终端的接入。它具有网络管理、测试和性能监控功能，能使用户的每一个设备具有唯一的地址，并解决多个用户设备使用总线时的优先级别问题。注意，NT1 用于接入数字设备，计算机必须装

有 ISDN 适配卡。

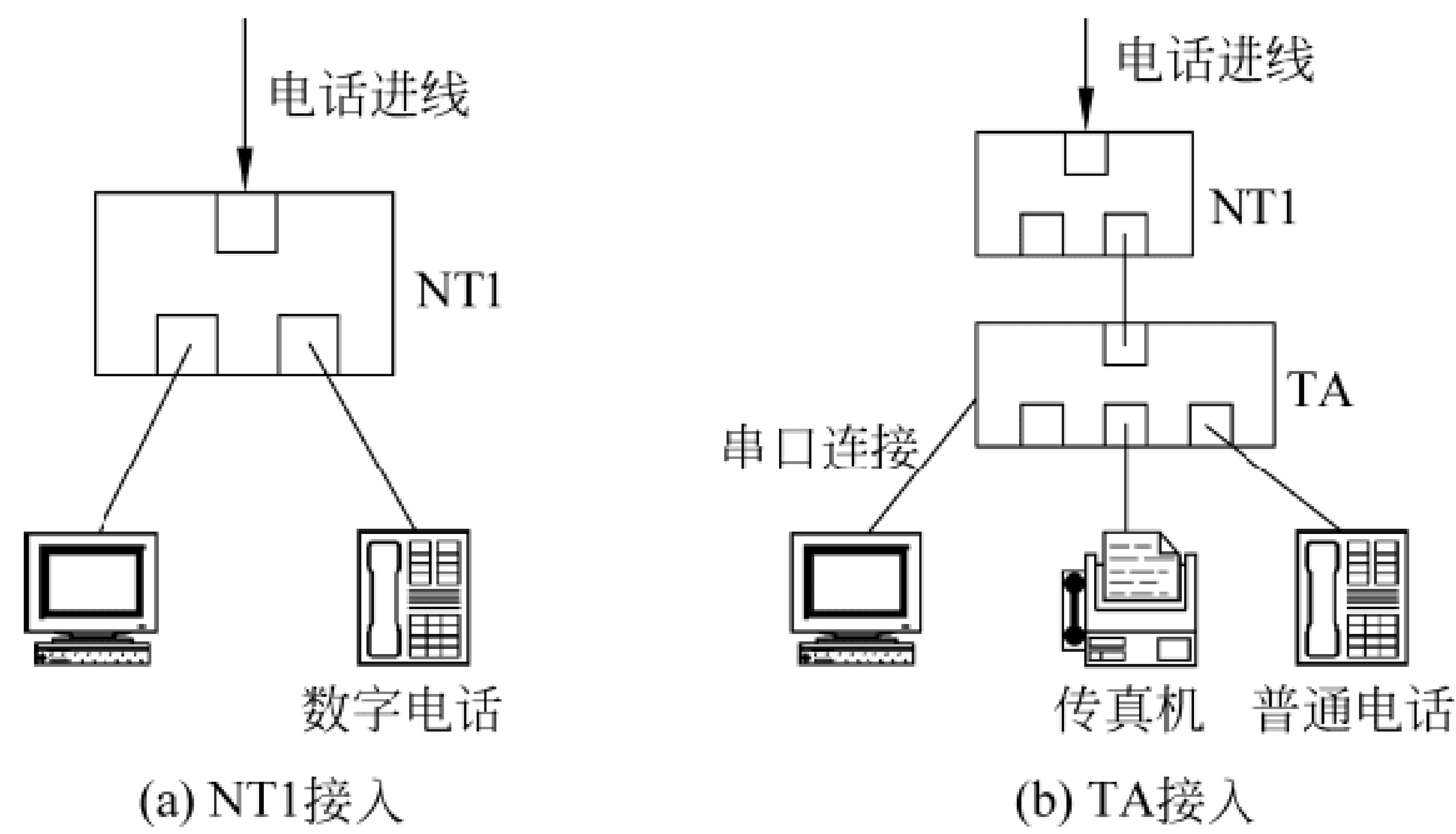


图 6.12　ISDN 的两种基本接入方式

对于大一些的单位，NT1 就不够用了，需要一个 ISDN 专用的小交换机 PBX——NT2。NT2 是一次群速率接口终端，向用户提供 3B+D 的四线双向传输能力，它至少覆盖 OSI 的下 3 层。

2）ISDN 终端适配器

ISDN 终端适配器的功能是使现有的非 ISDN 标准终端（如模拟电话、G3 传真机、PC 的串口等）能够使用 ISDN，为用户在现有终端上提供 ISDN 业务。ISDN 终端适配器分为内置和外置两种。内置 ISDN 终端适配器俗称 ISDN 适配卡，外置 ISDN 终端适配器俗称 ISDN TA。通常大部分 ISDN 终端适配器具有两个信道通信能力。与计算机的连接有串口与并口两种方式：串口方式的最高速率为 112.5Mbps，并口的最高速率为 128Mbps。ISDN TA 除具有 ISDN 卡的功能外，还提供两种模拟接口，即有一个 ISDN 接口、三个用户接口——两个 RJ-11 的普通模拟电话接口，一个可以通过电缆连接计算机的 RS -232D 接口。

6.2.2　非对称数字线路

1．数字用户线路

非对称数字线路（ADSL）是数字用户线（Digital Subscriber Line，DSL）的一种。DSL 是以铜电话线为传输介质的、点对点的接入技术系列，也称 *x*DSL。DSL 技术系列的宗旨是通过电子设备和软件，使现有的电话线作为数字传输线，并使带宽至少达到 2Mbps，而现有技术仅能使铜质电话线以 28.8kbps（辅以软件可达 56.3kbps）的速率传输语音信号。几种主要的 *x*DSL 技术如表 6.4 所示。

表 6.4　几种主要的 *x*DSL 技术

类型		线对数	上行/下行速率（Mbps）	最大传输距离（m）
对称 DSL	SDSL（Symmetric DSL，单线/对称数字用户线）	1	1/1	3300
	HDSL（High-bit-rate DSL,高比特率数字用户线）	2～3	1.533/1.533	3700
非对称 DSL	ADSL（Asymmetric DSL,非对称数字用户线）	1	1.5/8	5500
	VADSL(超高比特率数字用户线)	1	2.3/5.1～51	300～1500

目前最常用的是 ADSL。

2. ADSL 概述

ADSL 是非对称传输率的数字传输线技术，适合于作接入技术。ADSL 技术使得两个 Modem 之间的电话线上产生 3 个信息通道：

- 一条 1.5～9Mbps 的高速下行通道；
- 一条 16kbps～1Mbps 的中速双工信道；
- 一条普通电话服务 POST 通道（3kHz），一旦 ADSL 失效，还可以使用 POST。

高速和中速信道都可以被多路低速信道复用。为了建立多重频道的传输方式，ADSL 采用 FDM 和 Echo Cancellation 两种方法分离出不同频宽。

ADSL 能够在现有电话双绞线上提供 8Mbps 的高速下行速率和 1Mbps 的上行速率，有效传输距离可达 5km，非常适合双向带宽要求不一致的应用，如 Web 浏览、多媒体点播、消息发布等。

如图 6.13 所示，ADSL 接入模型主要由中央交换局端模块和远端模块组成。

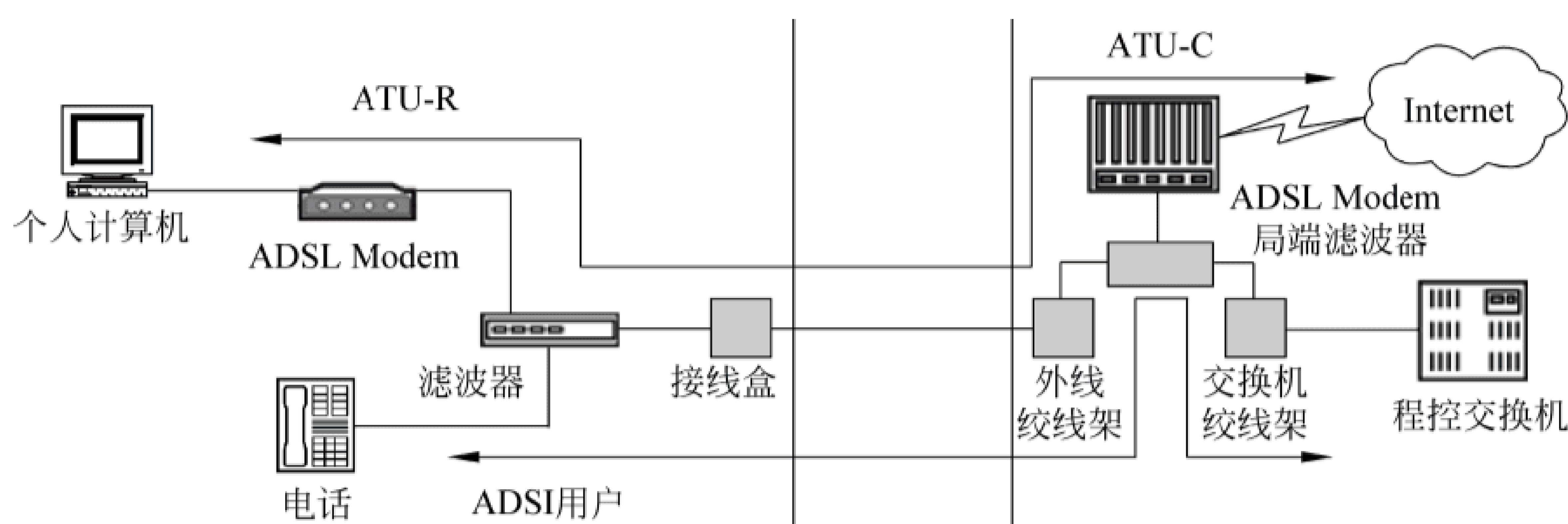


图 6.13　ADSL 的接入模型

中央交换局端模块包括在中心位置的 ADSL Modem 和接入多路复合系统。处于中心位置的 ADSL Modem 被称为 ATU-C（ADSL Transmission Unit-Central）。接入多路复合系统中心 Modem 通常被组合成一个被称作接入结点，也被称作 DSLAM（DSL Access Multiplexer）。远端模块由用户 ADSL Modem 和滤波器组成。用户端 ADSL Modem 通常被称为 ATU-R（ADSL Transmission Unit-Remote）。

3. ADSL 用户端安装

对普通用户来说，安装用户端 ADSL 时，只要将电话线连上分离器，分离器与 ADSL Modem 之间用一条两芯电话线连上，ADSL Modem 与计算机网卡之间用一条双绞网线连通即可完成硬件安装，如图 6.14（a）所示。在硬件安装好之后，再将 TCP/IP 中的 IP、DNS 和网关参数项设置好，便完成了安装工作。对局域网用户来说，ADSL 安装只需用直连网线将集线器/交换机与 ADSL Modem 连起来就可以了，如图 6.14（b）所示。

4. ADSL 接入类型

（1）虚拟拨号入网方式：并非是真正的电话拨号，而是用户输入账号、密码，通过身

份验证，获得一个动态的 IP 地址，可以掌握上网的主动性。使用拨号入网方式工作，还需要安装相应的拨号软件。

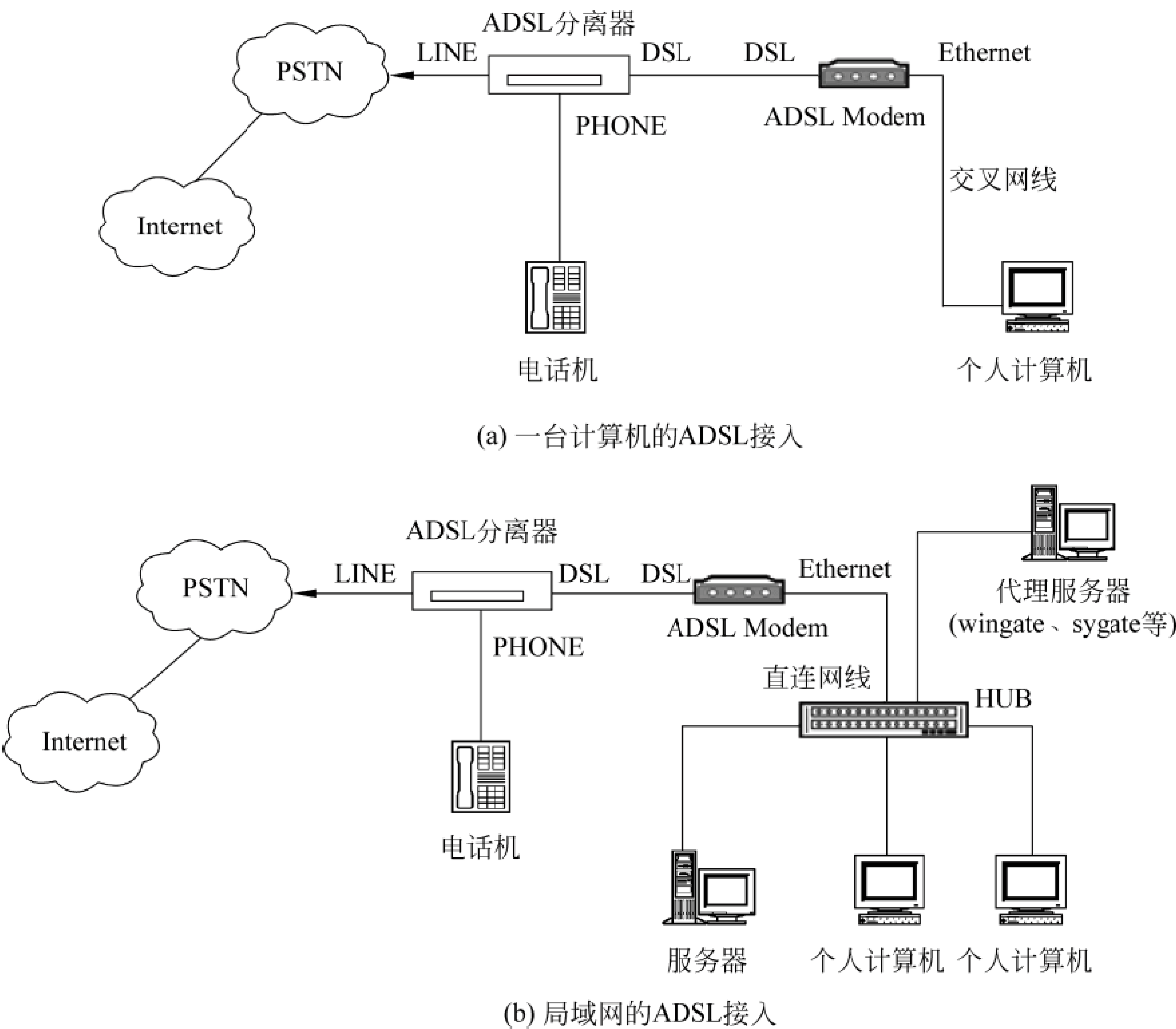


图 6.14　ADSL 接入

（2）专线入网方式：用户拥有固定的静态的 Internet 地址（IP 地址），不需要拨号，开机即可连通上网。

6.3　光 纤 接 入

6.3.1　光纤接入网概述

1．光纤接入网及其结构

以光纤作为传输媒介，并利用光波作为光载波传送信号的接入网，称为光纤接入网（Optical Access Network，OAN），又称为光纤用户环路（Fiber In The Loop，FITL）。如图 6.15 所示为一个光纤接入网示意图。由图中可以看出，光纤接入网除了包括光纤介质外，还包括远端设备——光网络单元（Optical Network Unit，ONU）或光网络终端（Optical Network Terminal，ONT）、局端设备——光线路终端（optical line terminal，OLT）。

（1）OLT 的作用是为接入网提供与本地交换机之间的接口，通过光传输与用户端的光网络单元通信，并提供对自身和用户端的维护和监控。

（2）ONU 的作用是为接入网提供用户侧的接口。它的主要功能有：

- 终结来自 OLT 的光纤；
- 处理光信号，为多个小企业、事业用户和居民住宅用户提供业务接口，接入多种用户终端；

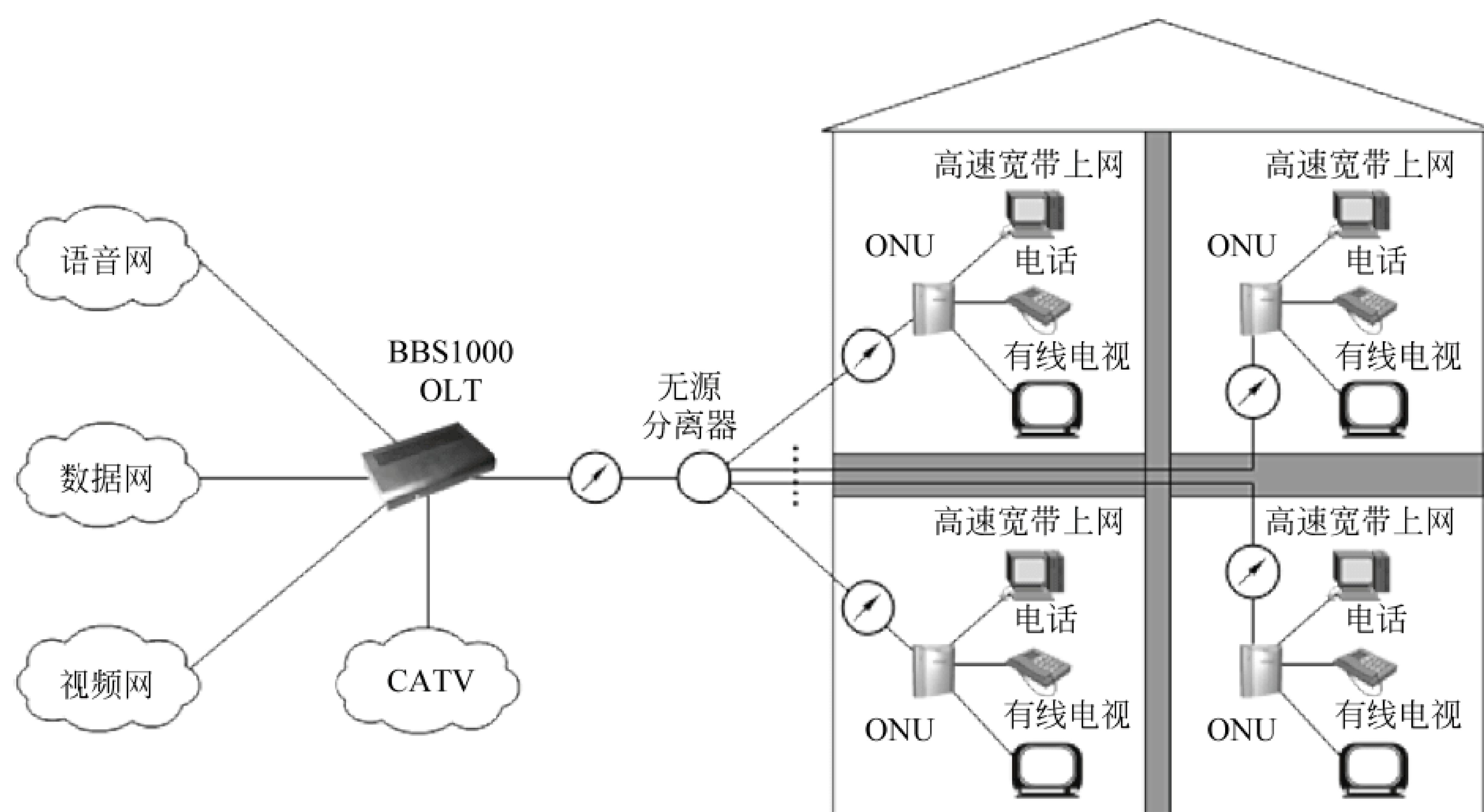


图 6.15　光纤接入网结构

- 光/电和电/光转换，因为 ONU 的网络端是光接口，而其用户端是电接口；
- 对语音的数/模和模/数转换；
- 相应的维护和监控功能。

2．光纤接入网分类

（1）根据 ONU/ONT 的放置位置，光纤接入可以分为如下几种类型：

- 光纤到户（Fiber To The Home，FTTH）；
- 光纤到邻里（Fiber To The Neighbor，FTTN）；
- 光纤到办公室（Fiber To The Office，FTTO）；
- 光纤到楼层（Fiber To The Floor，FTTF）；
- 光纤到大楼（Fiber To The Building，FTTB）；
- 光纤到路边（Fiber To The Curb，FTTC）；
- 光纤到小区（Fiber To The Zone，FTTZ）；
- 光纤到远端单元（Fiber To The Remote Unit，FTTR）。

（2）从系统分配上光纤接入网（OAN）分为有源光网络（Active Optical Network，AON）和无源光网络（Passive Optical Network，PON）两类。PON 是指 ODN（光配线网）中不含有任何电子器件及电子电源，全部由光分路器（splitter）等无源器件组成，不需要贵重的有源电子设备。PON 网络的突出优点是消除了户外的有源设备，所有的信号处理功能均由交换机和用户宅内设备完成。而且这种接入方式的前期投资小，大部分资金可以等到用户真正接入时才投入。虽然它的传输距离比有源光纤接入系统的短，覆盖的范围较小，但它造价低，无须另设机房，维护容易。因此，这种结构可以经济地为居家用户服务。

（3）按照拓扑结构，光纤接入网有 3 种基本类型：总线型、环形和星形。由此又可派生出总线-星形、双星形、双环形、总线-总线型等多种组合应用形式。

6.3.2　光纤到户及其应用

目前应用最多的光纤接入是光纤到户。严格的“光纤到户”是 FTTH。但是，现在通常也把 FTTB、FTTC、FTTN 也称为光纤到户。由于实际的光纤到户包括了上述 3 种情况，所以人们也用 FTTx 来总称广义的“光纤到户”。下面介绍两种 FTTH 方案。

1．交换以太网 FTTH

传统以太网都是采用电信号。为此，可以在用户端使用一个单纯的光/电或电/光转换器——MC（Media Converter），就可以实现 FTTH 接入，而不必更换支持光纤传输的网卡。如图 6.16 所示为这种方案的结构。

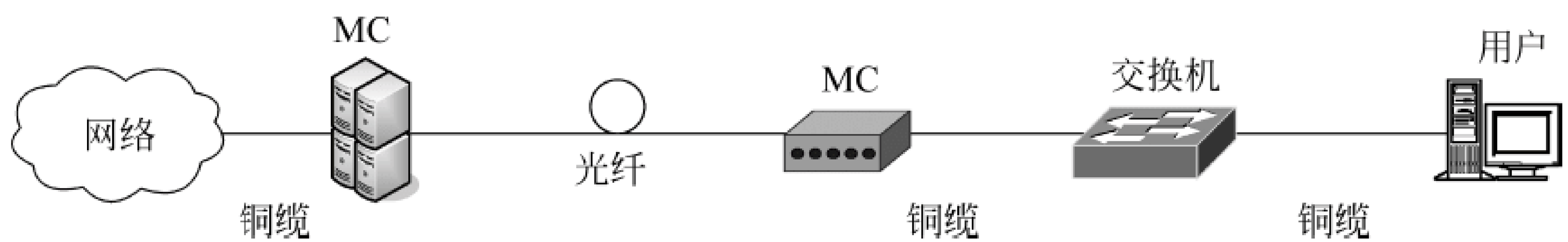


图 6.16　MC+传统以太网交换机实现 FTTH 接入

2．光纤以太网方式 FTTH

光纤以太网方式的 FTTH 如图 6.17 所示。这里使用了具有光接口的以太网交换机，也可以是新的符合 IEEE 802.3ah 规范的光以太网接入设备。根据 IEEE 802.3ah 的规定，接入网所采用的光以太网技术应采用单纤双向传输方式，上下行采用 WDM 方式分别使用不同的波长进行传输，上行使用 1310nm 波长，下行使用 1550nm 波长。

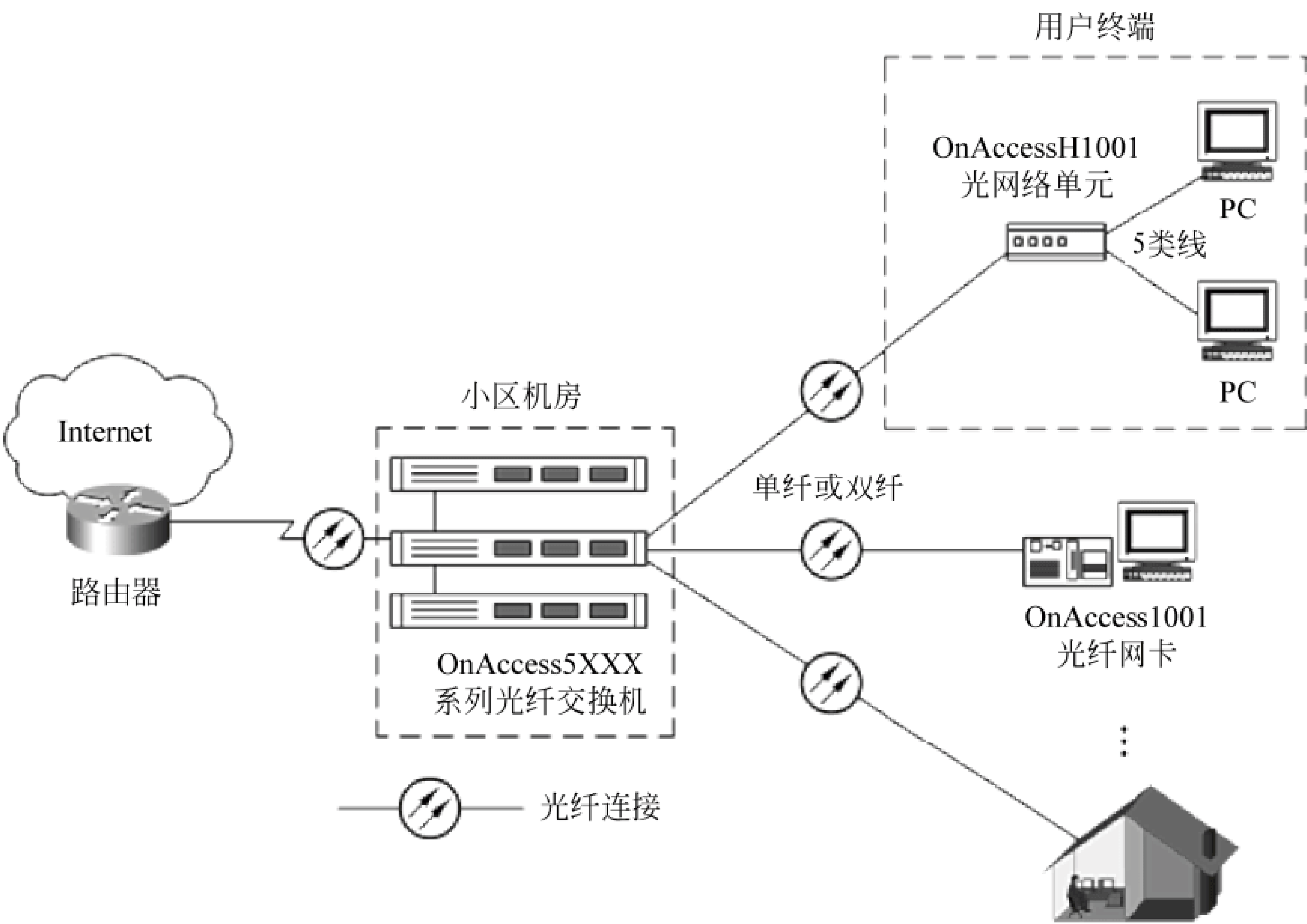


图 6.17　光纤以太网方式的 FTTH

6.4　光纤/铜线混合接入网

6.4.1　HFC 系统结构

光纤/铜线混合接入网络（Hybrid Fiber/Coax，HFC）技术是在传统的同轴电缆 CATV 技术基础上发展起来的。CATV 最初的意思是公用天线（community antenna television）系统，20 世纪 80 年代后在此基础上发展为有线电视（cable television）。CATV 技术的要点是在有线电视台的前端把电视图像用光纤和同轴电缆组合起来的方式（主干线路用光纤，在 ONU——光接点之后，即进入各家各户的最后一段线路用同轴电缆）传送到各家各户。但是，这种系统是单向的，只有下行。HFC 的目的是在此基础上实现双向传输。

6.4.2　HFC 的频谱结构和传输模式

1．HFC 的频谱结构

上行回传信号要选择与下行频段分开的频段，各位于不同的频谱上，实行频分复用。如图 6.18 所示为 HFC 系统频谱结构。

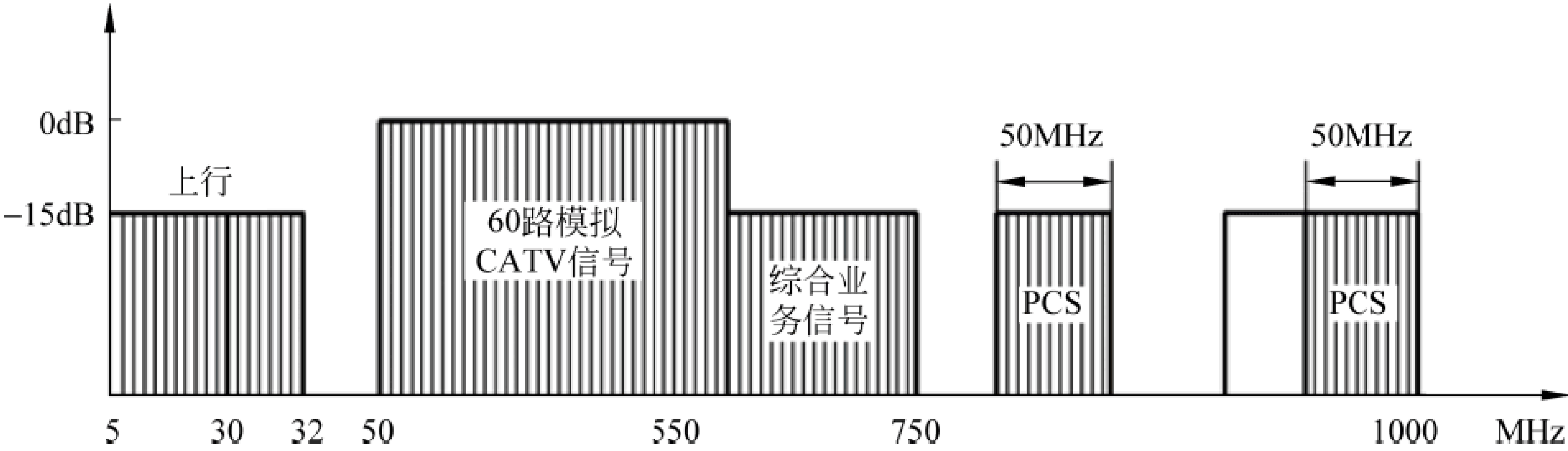


图 6.18　HFC 系统频谱结构

如表 6.5 所示为我国接入网总技术规范中所定义的频段划分。

表 6.5　HFC 频段的划分

波　段	频带（MHz）	业　务
R	5.00～30.0	上行电视及非广播业务
R1	30.0～32.0	上行非广播业务
I	38.5～92.0	模拟广播电视
FM	87.0～108.0	调频立体声广播
A1	111.0～167.0	模拟广播电视
III	167.0～223.0	模拟广播电视
A2	223.0～295.0	模拟广播电视
B	295.0～337.0	模拟广播电视
IV	350.0～550.0	数字或模拟广播电视
V	550.0～710.0	数字电视和 VOD 等

续表

波　段	频带（MHz）	业　务
VI	710.0～750.0	非广播业务
VII	750.0～1 000.0	个人通信

2．HFC 的传输模式

Cable Modem 的传输模式分为对称式传输和非对称式传输。

1）对称式传输

对称式传输是指上/下行信号各占用一个普通频道 8MHz 的带宽，上/下行信号可能采用不同的调制方法，但采用相同传输速率（2～10Mbps）的传输模式。在有线电视网里利用 5～30（32）MHz 作为上行频带，对应的回传最多可利用 3 个标准 8MHz 频带：500～550MHz 传输模拟电视信号，550～650MHz 为 VOD（视频点播），650～750MHz 为数据通信。利用对称式传输，开通一个上行通道（中心频率 26MHz）和一个下行通道（中心频率 251MHz）。上行的 26MHz 信号经双向滤波器检出，输入给变频器，变频器解出上行信号的中频（36～33MHz）再调制为下行的 251MHz，构成一个逻辑环路，从而实现了有线电视网双向交互的物理链路。

2）非对称式传输

由于用户上网发出请求的信息量远远小于信息下行量，而上行通道又远远小于下行通道，人们发现非对称式传输能满足客户的要求，而又避开了上行通道带宽相对不足的矛盾。

6.4.3　Cable Modem 模式

Cable Modem（电缆 Modem）是利用 HFC 接入网进行高速访问的一种重要的通信设备。它不仅可以提供对 Internet 的高速访问，还可以提供音频、视频、访问 CD-ROM 等服务，并且具有很高的接入速率，理论上下行速率可达 36Mbps，上行速率可达 10Mbps。

如图 6.19 所示为 Cable Modem 的内部结构。Cable Modem 本身不是单纯的调制解调器，它也是一个调谐器（将数字信道同模拟电视信道分离）和加密设备，同时还起到路由和网卡的部分作用。

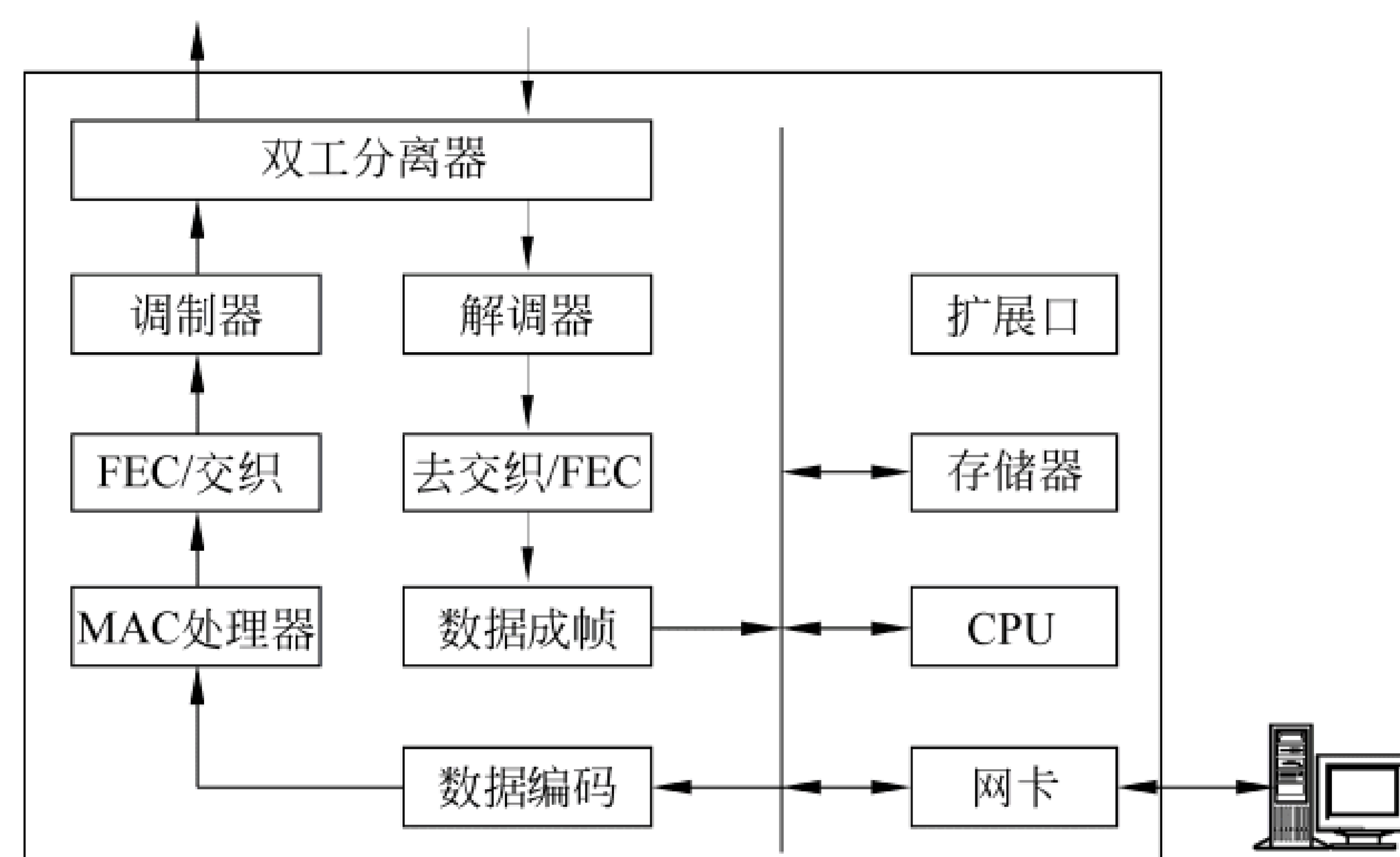


图 6.19　Cable Modem 的内部结构

1．从传输方式的角度

（1）双向对称式传输：传输速率为 2～3Mbps，最高能达到 10Mbps。

（2）非对称式传输 Cable Modem：传输下行速率为 30Mbps，上行速率为 500kbps～2.56Mbps。

2．从数据传输方向角度

（1）单向 Cable Modem：指本身不支持把数字信号转换成模拟信号，不能上传数据。

（2）双向 Cable Modem：可以把数字信号转换成模拟信号，也可以把模拟信号转换成数字信号；既可以上传数据，也可以下载数据。

3．从网络通信角度

（1）同步（共享）Cable Modem：类似于以太网，网络用户共享同样的带宽。当用户增加到一定数量时，其速率急剧下降，碰撞增加，登录入网困难。

（2）异步（交换）Cable Modem：ATM 技术与非对称传输正在成为技术的发展主流趋势。

4．从接入角度

（1）个人 Cable Modem：用于接入单机。

（2）宽带 Cable Modem（多用户）：可以将一个计算机局域网接入。

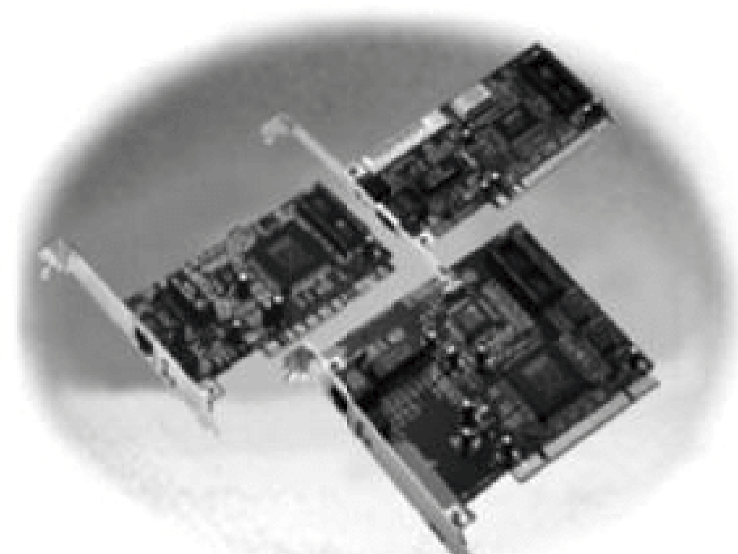
5．从接口角度

（1）外置式 Cable Modem：如图 6.20（a）所示，它是一个盒子，计算机连接 Cable Modem 前需要添置一块网卡，可以支持局域网上的多台计算机同时上网。

（2）内置式 Cable Modem：如图 6.20（b）所示，它是一块 PCI 插卡，只能用在台式计算机上，Macintosh 计算机和笔记本计算机无法使用。

（3）交互式机顶盒：主要功能是在频率数量不变的情况下提供更多的电视频道。通过使用数字电视编码（DVB），交互式机顶盒提供一个回路，使用户可以直接在电视屏幕上访问网络，收发 E-mail 等。如图 6.20（c）所示为交互式机顶盒示例。


(a) 外置式Cable Modem


(b) 内置式Cable Modem


(c) 交互式机顶盒

图 6.20　Cable Modem 的外形

6．按照用户类型

（1）CMP（Cable Modem Personal）：适合个人用户，是具有全面的媒体访问控制层

（MAC）桥接功能、传送和接收数据功能，可以即插即入的 Cable Modem。

（2）CMW（Cable Modem Workgroup）：适合中小企业和多家庭使用，最多可以支持 3 个用户，每个用户均可以获得 CMP 功能。

（3）CMB（Cable Modem Business）：适合于企业网、学校系统、政府机关等使用，可以连接大量的用户，使每个用户均获得 CMP 功能，并可以根据不同的访问和操作安全性要求实现保护。

6.5 无 线 接 入

6.5.1 无线接入概述

无线接入网是以无线技术（包括移动通信、无绳电话、微波、卫星通信等）为传输手段，连接起局端至用户间的通信网，向用户提供各种通信业务。

无线接入种类繁多，并且可以用不同的方法进行分类。按应用方式分类有固定终端无线接入、移动终端接入和有线综合接入。

1. 固定终端无线接入

（1）单区制无线接入，是传统的无线接入方式，一般采用 150MHz、350MHz 和 800MHz 频段，适合用户较少的郊区或农村使用，覆盖半径可达几万米。

（2）微波点对多点通信系统（Multiple Access Radio System，MARS），又称一点多址微波通信系统，由一个基站可以向几十户端站传送信息，传送频率为 1.3～2.5GHz，经过中继后总覆盖半径可达 150km 以上，适合于小集中、大分散的用户地区。可用于供电话、传真、低速数据、窄带 ISDN 等业务。

（3）本地多点分布业务（Local Multipoint Distribution Service，LMDS）系统，使用频段为 2.8GHz 左右，传输距离为 1～8km，可与固定卫星链路连接，传输宽带业务：高速数据、广播电视、视频点播和电话业务。主要缺点是有阻塞，且传输质量受天气变化影响。

（4）多点多路分布业务（Multipoint Multichannel Distribution Service，MMDS），使用频段为 2.5GHz，业务与 LMDS 相似，可有 33 个模拟电视电路，在发射天线周围 50km 范围内可将多路数字电视信号直接送到用户。

（5）固定蜂窝和微蜂窝（无绳通信）接入系统，将移动终端改为固定终端后，时变性和随机性减小，随着用户间干扰减小，容量可以增加，传输距离可以加大。美国摩托罗拉公司开发的 Will CDMA 无线用户环路系统，是一种代表性产品，采用 V5.2 接口，使用载波频率 800MHz、900MHz 或 1.8GHz、1.9GHz。

（6）甚小孔径终端卫星（Very Small Aperture Terminal，VSAT）系统，是工作波段为 C 或 Ku 波段、地球站天线直径一般小于 2.3m 的卫星通信系统，一般用于小容量数据传输和小容量语音。

（7）卫星直播（Direct Broadband System，DBS）系统，即同步卫星电视广播系统。

（8）采用 C 或 Ku 波段的同步卫星通信（Synchronous Satellite Communication，SSC）

系统，为采用同步卫星上的转发器进行通信，工作波段为 C 或 Ku 波段，地球站天线直径一般大于 6m 的卫星通信系统。

2．移动终端接入

（1）无线寻呼，即普通的 BP（Beep-Pager）机系统。
（2）无绳电话（Cordless Telephone，CT）系统。
（3）集群通信系统，主要用于生产、管理、交通、公安、消防等系统。
（4）蜂窝移动通信接入系统。
（5）同步卫星通信系统。
（6）公共陆地移动通信系统（Future Public Land Mobile Telephone System，FPLMTS）。

3．有线无线综合接入

（1）光纤无线混合（Hybrid Fiber & Wireless，HFW）系统。
（2）个人通信系统（Personal Communication System，PCS）。
上述应用类型，从技术上说，大体上可以归为基于卫星通信的技术、基于数字微波通信的技术和基于移动通信的技术。

4. 常用宽带无线接入制式

下面介绍几种常用宽带无线接入制式，如表 6.6 所示。

表 6.6　几种常用宽带无线接入制式

制式	接入带宽	组网方式	特点
固定无线本地分配业务 LMDS	10G～30GHz	点对多点	频带宽、速率高 信道上使用 ATM/TDMA 等技术，动态分配带宽 提供多种业务
MMDS	5.5GHz	点对多点（共享系统） 点对点（专用带宽系统）	业务扩展灵活（可覆盖上千用户） 天线、馈线等接口开放，利于合作制造 业务包括 TDM、专线、IP 等
SDH 微波	155MHz 以上	点对点 适合干线或大客户	可支持各种业务 SDH 环网有自愈功能
PDH 微波	E1/3E1/8E1/16E1/2×16E1 接口	点对点	适合于 TDM 专线接入用户
扩频微波	有 E1 接口 以太网接口	视距无线点对点	抗干扰能力强 使用频率无须到管理部门备案
远红外通信系统	3×10^{11}MHz	10Base-T 接口 100Base-T 接口 155 OC3 接口 适合临时接入系统	单色性 方向性，保密性好 无辐射性 理论覆盖 2～3km，一般几百米
DVB 卫星通信	上行：128kbps 下行：2Mbps，3Mbps，8Mbps	长途传输	应用简单 系统造价与传输距离、地理环境无关
无线光纤	1～2Gbps	大容量用户点对点 城域网骨干结点间连接	可利用 SDH 环网自愈功能 灵活 可提供多种不同接口

6.5.2 卫星通信

1. 概述

卫星通信系统是利用人造地球卫星作为中继站，转发无线电信号，在多个地球站（地面站）之间进行的通信系统。

卫星通信具有覆盖面积大、多址通信、频带宽、信道稳定等特点。

（1）覆盖面积大。卫星通信覆盖面积大，并且不受地理条件和通信对象运动条件的限制，在电路使用费方面也不像地面微波中继系统那样因距离增加而投资增加。

（2）多址通信。一颗卫星可以与多个地球站进行通信。

（3）频带宽、容量大。现在，通信卫星的传输频带可以达到 500MHz，即可以传输 10 万路以上的电话信号，超过以往的任何通信方式。

（4）信道稳定。卫星通信使用的是微波频段，但与地面微波中继通信不同。地面微波中继信号电磁波主要在大气层中传输，受大气折射和地面反射影响，有较严重的衰减现象。卫星通信的电磁波主要在大气之外的宇宙空间传输，因此电磁波较稳定。

（5）缺点：检修困难、时延较大。由于卫星发射之后，很难检修，要求卫星必须具有高可靠性和长寿命。同时，由于传输距离长，信号的时延就会大。从一个地球站发射信号到卫星再到另一个地球站，通信距离为 72 000km。双向通信往返共约 133 000km，即使传输速度为光速，也需 0.5s。

2. 卫星通信系统的组成与工作过程

卫星通信系统主要由通信卫星和地球站组成。

1）通信卫星

通信卫星是卫星通信系统中的转发器，它用来接收从各地球站发来的信号，经频率变换和放大，再发送给别的地球站。它主要由位置和姿态控制系统、天线系统（包括双工器）、通信系统、遥测指令系统、电源系统和温控系统组成。

2）地球站

为了进行双向通信，每个地球站都有发射和接收设备。由于收发设备共用一副天线，为了分开收、发信号，在天线与收、发设备连接处装有双工器。发射设备由多路复用设备、调制器和发射机组成。接收设备由接收机、解调器和多路分解设备组成。如图 6.21 所示为卫星通信系统的组成以及工作过程。

下面说明 A 地球站与 B 地球站的通话过程：

（1）A 发射上行信号 f_1，到达卫星转发器；

（2）卫星转发器进行频率变换：先将 f_1 转换为频率较低的中频信号，放大，再转换为下行信号 f_2，经发射设备的输出功率放大器和天线发射至地球站；

（3）f_2 经地球站 B 的天线、双工器、低噪声放大器，进入下变频器，变频成中频信号，送到解调器恢复成基带信号。

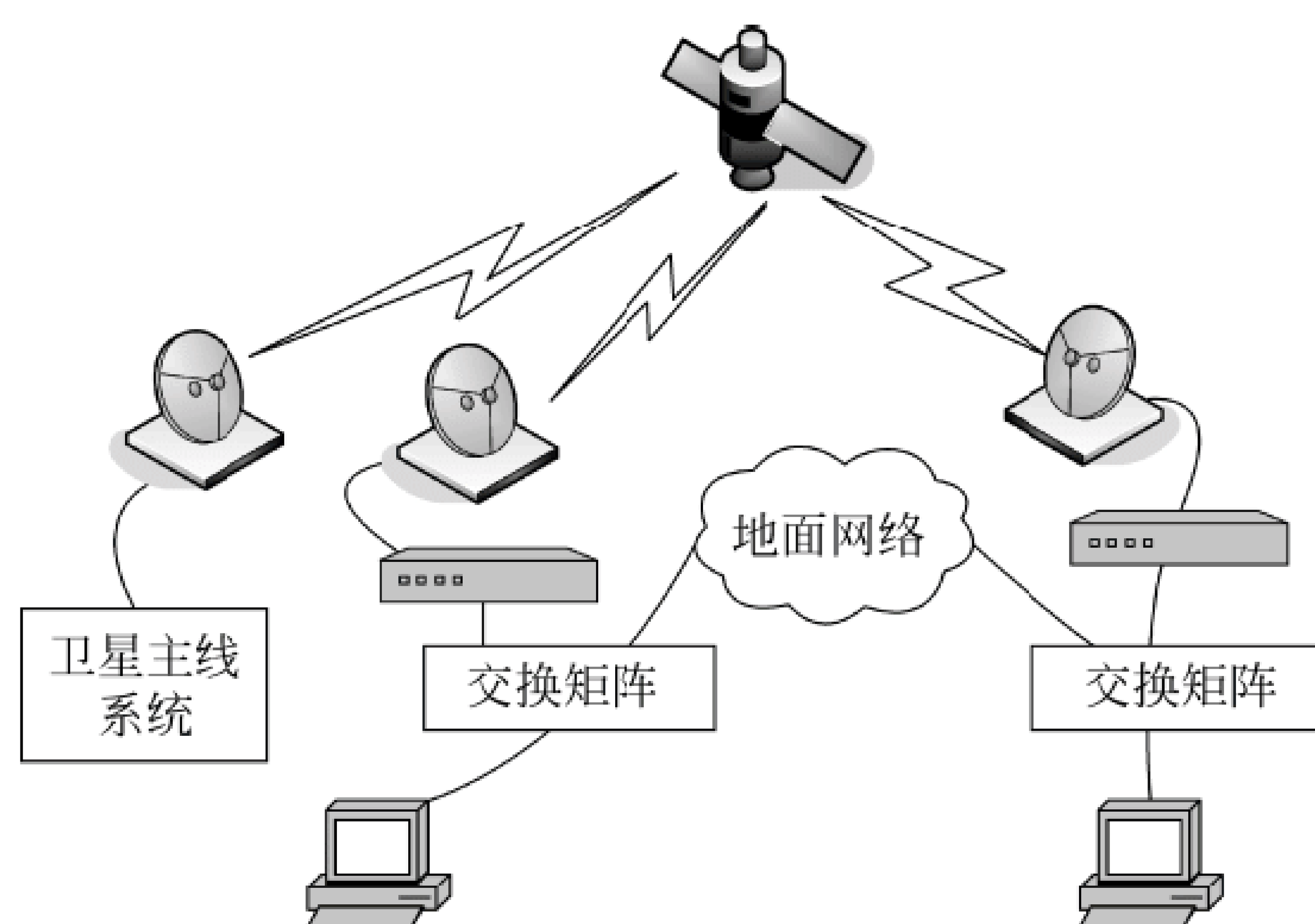


图 6.21　卫星通信系统的组成以及工作过程

3．卫星通信的多址方式

多址方式是指在卫星覆盖区内的一个地球站，通过一颗卫星的中继，可以与多个地球站通信，为此卫星转发器必须能分辨接收到的多路信号的来源，同时各地球站也要能从卫星发出的众多信号中区分出哪些信号是发给自己的。解决这个问题的办法称为多址技术。实现多址连接的基本理论是信号分割技术。目前，主要的多址技术有频分多址、时分多址、码分多址和空分多址。如图 6.22 所示为频分多址方式的示意图。其中，F_1、f_2；F_2、f_2；F_3、f_3 分别为 3 个移动终端的下行、上行信道频率。

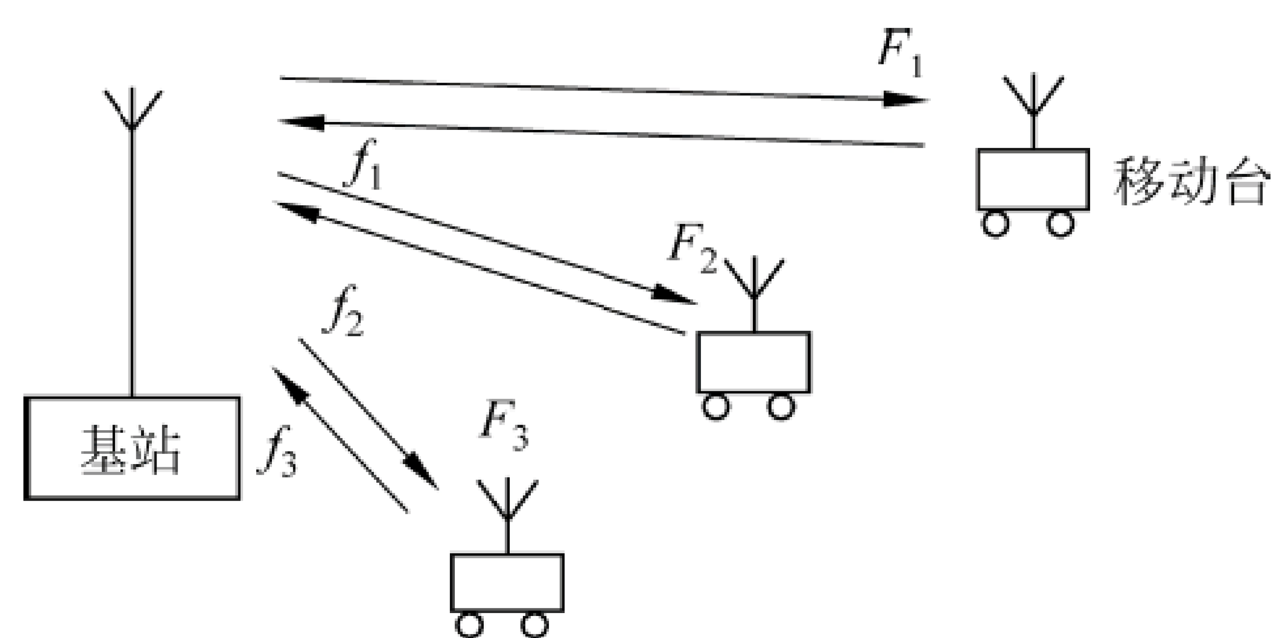


图 6.22　频分多址方式的示意图

4．卫星通信系统的类型

1）同步卫星通信系统

同步卫星通信系统使用距离为 36 000km 的静止轨道（同步轨道）卫星，有 3 颗卫星就可以覆盖全球。典型的 Internet IV 卫星系统，设置 38 个 C 波段转发器，10 个 Ku 波段转发器，可以转发 60 路电视和 5.3 万路电话信号，若采用星上交换、时分多址技术和数字电路倍增技术，总容量可达 12 万路。

2）甚小孔径天线地球站（VSAT）通信系统

VSAT 系统指天线口径很小（小于 2.3m）、高度智能化的地球站。目前 C 波段 VSAT 天线口径在 1m 以下，Ku 波段小于 2.3m。VSAT 卫星通信系统的优点是：成本低、体积小、智能化、高可靠、信道利用率高、安装维护方便，特别适合业务量小的地区。主要业务是传输数据和语音。

6.6 新一代接入技术：BPL 和 VLC

光纤接入和铜线接入需要较大投资，无线接入却有一定的辐射。当前，既没有辐射，也基本不需要说明投资的接入技术已经浮出水面。这就是 BPL（Broadband over Power Lines，电力线宽带）和 VLC（Visible Light Communication，可见光通信）。

6.6.1 BPL 接入

1. BPL 概述

BPL 也称高速电力线路通信，它是利用电力线传输数据、话音、视频信号的一种通信方式。通过连接在计算机上的电力 Modem（俗称“电力猫”），插入家中任何一个电源插座，即可实现最高 14Mbps 的上网速度。

BPL 起源于 20 世纪 40 年代的电力网载波通信（Power Line Communication，PLC）。当时用于电力系统调度中的通信，以节省单独敷设通信线路的开支。但是那是窄带的，并且有相当大的噪声。到了 20 世纪 90 年代初，随着国际互联网的普及，人们在 PLC 的基础上，开始了 SPL 技术的实验研究。包括 Google 在内的一些公司已经察觉到了这个宽带商机，正在向这项新技术投入资金。目前全球已有 100 个左右的相关测试项目正在进行，其中三分之一的项目在美国，其余大部分位于欧洲。上网用户数已经超过 17 万。

现在市场上的高速电力线通信设备的通信带宽，根据使用的协议和核心芯片的不同，通常有 2M、14M、45M 等多种标准。从承载业务能力、投资经济性和成熟度上进行综合比较，14M 产品应该说是发展的主流，也是目前得到应用最多的产品。

2. PLC 的关键技术

目前有两种 PLC 系统：一种是室内接入方式，它利用建筑物内的电源系统传输计算机和其他家庭电子设施间的信息；另一种是利用室外中等水平的电压线传输高速通信信号。通过互联网或邻居接入，通过低电压电力线或 Wi-Fi 连接分配到每个家庭。

从功能上看，PLC 系统可以分成 3 个子系统：PLCISS（PLC-based Integrated Services Systems）宽带接入子系统、PLCISS 软交换核心子系统和 PLCISS 增值业务子系统。整个体系架构在设计上遵循下一代网络（Next Generation Network，NGN）分层、全开放的体系架构，具有方便灵活、层次清晰、标准化程度高、易于扩展的优点。

PLC 涉及的主要技术有信号调制解调技术、媒体访问控制技术以及链路层的 QoS 保证机制。从实现的角度看，PLC 主要有如下几个关键技术环节。

（1）电力系统自身的噪声干扰问题。与专用的通信线路相比，在电力线上进行数据传递存在很多额外的干扰因素，如各种电气设备的启动以及运行状态的调整、线路上各种开关的闭合和打开等，都会给电力线路注入较大的干扰信号，导致供电线路上信号传输时，信噪比极低，信号难以提取。针对以上问题，通常高速电力线接入设备在设计的时候均进行了特殊的考虑，并对产品进行了大量的实验。解决干扰问题主要依靠选择合适的调制技

术。传统的调制技术，如 ASK、PSK 或 FSK 都不适用于这样的通信环境，必须采用特殊的调制技术。

（2）电磁性的影响问题。数据载波本身就是一种电磁波，而电力网使用的大多是非屏蔽线，用它来传输数据不可避免地会形成电磁辐射，这会影响数据的保密性。

（3）数据信号翻越电表和变压器问题。所谓翻越变压器，是指电力变压器都是针对工频设计的，而载波信号的频率都比工频高，因此数据信号经过变压器时会因较大的能量损失而迅速衰减失真。所谓翻越电表，指的是两个高速电力线通信产品通信的线路上经过了电表。因为电表的种类很多，呈现的滤波特性也差别很大，有些电表对电力线通信几乎没有任何影响，有些电表则对电力线通信所用的频段衰耗很大，通信信号不能很好地跨过电表。

这些技术难点最近都有比较好的解决。

3. PLC MODEM

PLC MODEM 即电力调制解调器，俗称电力猫。目前电力猫种类繁多，有多种分类方法。

（1）按照传输速率，可以分为 200M 电力猫、500M 电力猫和千兆电力猫等。

（2）按照传输媒介，可以分为有线电力猫和无线电力猫（Wi-Fi 电力猫）。

（3）按照功能，可以分为普通电力猫（不带拨号功能的电力猫）和拨号（PPPoE）电力猫（带拨号功能的电力猫）。

（4）按照接口，可以分为单多口电力猫和多口电力猫。主猫最少有一个网线接口，用于连接 ADSL 猫、光猫、路由器或者交换机出来的网线；有的主猫还会带一个局域网端口（LAN 口），可以在这个口上直接连接路由器、交换机或者计算机，这样的主猫多数是一个小小的路由器了，只不过这个路由器会同时将网络信号转换成电力线信号发送到强电线路上去。

表 6.7 为几种典型无线电力猫的性能比较。

表 6.7　几种典型无线电力猫的性能比较

产品型号	物理传输速度（Mbps）	电力线通信标准	有效传输速度（Mbps）		无线 Wi-Fi 传输速率（Mbps）	最大终端数量	网口数量
			TCP	UDP			
WPL-203	200	Home plug AV	:92	:92	300	63	3
PLQ-5100	500	Home plug AV	95	95	N/A	15	1
PWQ-5101	500	Home plug AV	90～93	92	150	15	1
PLS-8011	1000	G.hn	—	:350	N/A	15	1
PLQ-6031	1000	Home plug AV1.2	450	:500	N/A	63	1

4. 基于电力线的宽带接入方案

目前，DPL 的基本应用是将数据由本地变电站通过低电压配电网直接传输至用户家庭或中小型公司。图 6.23 为一种典型的 DPL 接入方案。

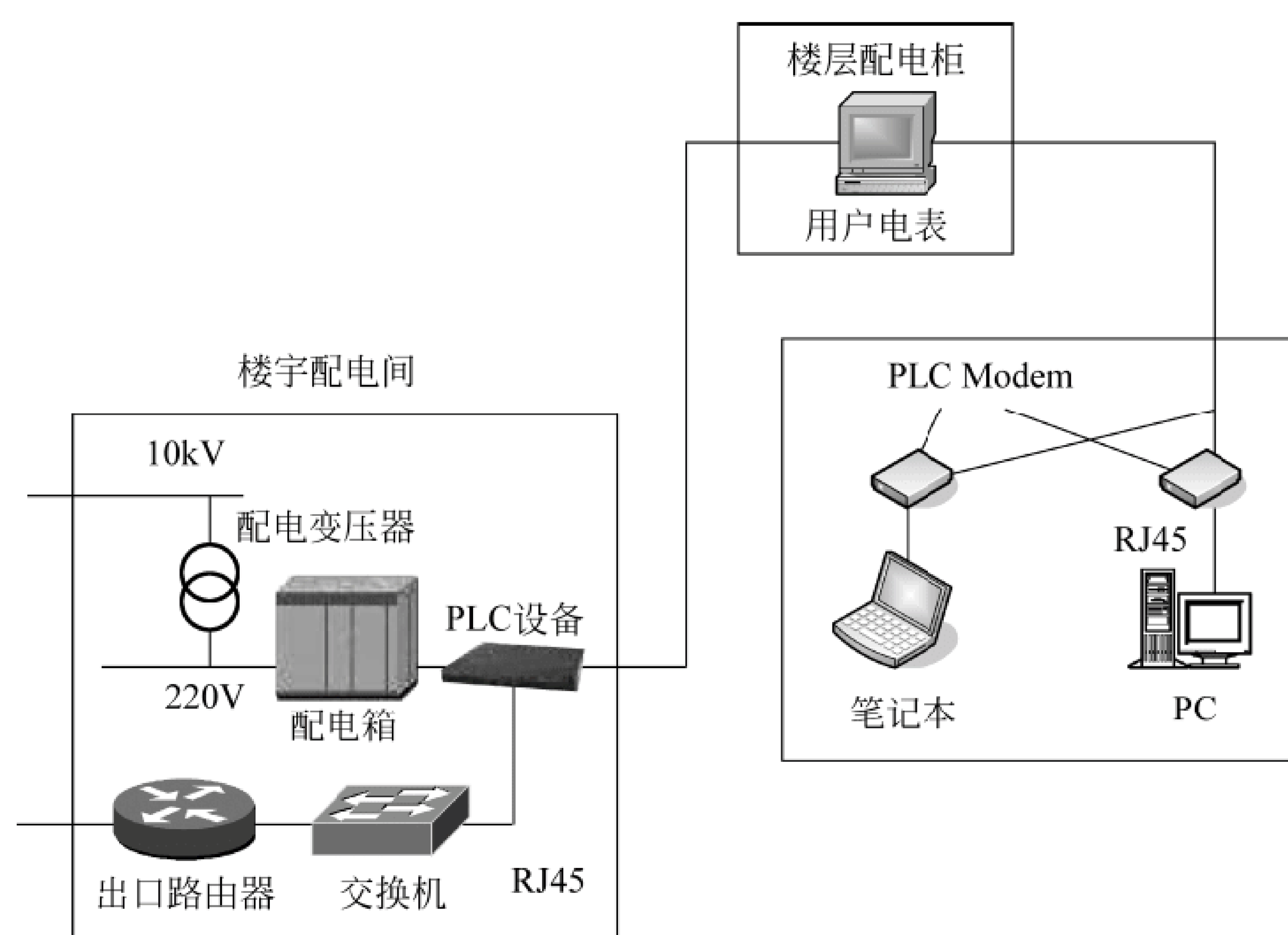


图 6.23　一种典型的 DPL 接入方案

6.6.2　VLC 接入

1. VLC 概述

一直以来，人们在一个人的头像顶上画一个闪亮的灯泡，被用来象征他的灵光乍现。然而真正由灯泡“点亮”发明创意的人，应当是德国物理学家哈拉尔德•哈斯（Herald Haas，见图 6.24），他将人们司空见惯的灯泡看作为一般人看不见的网络信号。2011 年，作为爱丁堡大学教授的他在 TED 上发表了一个演讲，宣布了他的一种专利技术：利用闪烁的灯光来传输数字信息，这个过程被称为可见光通信（VLC）。人们常把它亲切地称为 Li-Fi（Light Fidelity，可见光无线通信），以示它能与目前家喻户晓、广泛应用的 Wi-Fi 一样，可以为网络接入技术带来革命性的进步。

除了爱丁堡大学，德国的弗劳恩霍夫光电研究所、欧洲另一个团队在其操作的 ACEMIND 项目以及复旦大学计算机科学技术学院实验室都曾经实现过类似的技术。

目前，作为与 Li-Fi 相关的创业第一家公司——位于爱丁堡的 pureLifi 公司的第一代产品 Li-1st 已经可以实现 3m 内的双向传输，速度可达到 5Mbps，同时 LED 灯的照明功能不会受到任何影响。在 2014 第四季度，pureLiFi 上线了 Li-Fi 网络产品 Li-Flame，该系统可以实现把现成的灯泡转换成 Li-Fi 接入点，自动双向传输数据的功能。也就是说，只要拥有 Li-Flame，见到灯泡就可以上网。

Li-Flame 有两个关键的配件，如图 6.25 所示：上边是天花板套件，只需通过标准的以太网端口连接到 LED 灯具，就可以形成一个小范围多址切换的网络，同时 AP（Access Point，接入点）之间可以无缝切换。下边是桌面套件，通过 USB 接口连接到用户的设备，就可以利用红外线向天花板套件上传数据，速度可达到 10Mbps，可充电，当用户从一个 AP 转移到另一个时（比如进入另一个房间），可保证连接不断，增强用户移动性。



图 6.24　Herald Haas



图 6.25　Li-Flame

由于 VLC 有着广阔的前景，IEEE 在 2003 年开始并最终于年发布了 VLC 标准。这是 VLC 的第一个标准，包含了 3 个物理层类型，分别对应于低中高速数据传输。但是，由于缺少 LED 照明部门的参与，并没有给出 VLC 最终的标准。

近年来，国际红外数据协会（IrDA）和在 VLC 标准化工作中开展了一系列的合作。2009 年它们在 IrDA 标准的基础上发布了第一个 VLC 标准。在这个标准下，现有的 IrDA 光学模块可以在经过改造后被用于 VLC 的数据传输。

2. VLC 关键技术

1）高调制带宽的 LED 光源

目前商用白光设计的初衷是用于照明，而并非用于通信，所以其调制带宽有限，只有约 3～50MHz。为了进行通信就需要在保证大功率输出的前提下，开发出具有更高调制带宽的 LED 光源。

2）LED 的大电流驱动和非线性效应补偿技术

在 VLC 系统中，LED 需要进行大电流驱动。但是，LED 是一种非线性元件，电流增大会使可见光信号发生畸变。因此在实际使用中需要合理地控制偏置电压、信号动态范围、信号带宽等参数，并且根据的非线性传输曲线的特征有意识地对调制信号进行预畸变处理等等，以提高调制效率，提升传输容量。

3）光源的布局优化

在 VLC 系统中，白光光源需要同时实现室内照明和通信的双重功能。由于单个 LED 的发光强度比较小，因此实际系统中光源应采用多个 LED 组成的阵列。LED 阵列的布局是影响可见光通信系统性能的重要因素之一。一方面，要满足室内照明的要求；另一方面，需要考虑室内信噪比的分布，避免盲区和阴影的出现。一般来说，LED 的数目越大，室内的照明度越高，系统接收到的光信号的功率也越大，但由不同路径造成的符号间的干扰也越严重。因此，在对可见光通信系统的研究中，应对 LED 阵列进行合理的布局。

此外，对于不同的室内环境，如何迅速地建立光功率与信噪比分布模型，实现快速的智能布局也是可见光通信研究中需解决的关键问题。

4）光学 OFDM 技术

为了在有限带宽的条件下实现高速传输，极具吸引力的高频谱调制技术是 OFDM（Orthogonal Frequency Division Multiplexing，正交频分复用技术）。该技术将信道的可用带宽划分为许多个子信道，利用子信道间的正交性实现频分复用，并可以在子载波上通过对比特和功率的分配来实现信号传输对信道条件的调节适应，从而为信道色散提供了一个简单的解决方法。由于降低了子载波的传输速率，延长了码元周期，因此具有优良的抗多径效应性能。此外 OFDM 还可以使不同用户占用互不重叠的子载波集，从而实现下行链路的多用户传输。

5）光学 MIMO 技术

MIMO（Multiple-Input Multiple-Output，多个发射和多接收）可以使信号通过发射端与接收端的多个天线传送和接收，可以在不增加频谱资源和天线发射功率的情况下，成倍地提高系统信道容量，被视为下一代移动通信的核心技术。采用白光 LED 阵列对于 MIMO 技术也是非常有效的支持。

6）高灵敏度的广角接收技术

室内 VLC 大多数工作在直射光条件下，当室内有人走动或者在直射通道上有障碍物时，将会在接收机处形成阴影效应，影响通信性能，甚至出现通信盲区，使通信中断。采用大视场的广角光学接收系统可以解决这一问题，其大视场角的特性可以保证同时接收直射和散射光信号，这样就避免了“阴影”和“盲区”现象的发生。此外，接收光学系统的大视场特性可以解析出多个独立的通信信道，这对于室内 VLC 系统采用 MIMO 技术也是极大的支持。

7）消除码间干扰的技术

在室内 VLC 系统中，采用 LED 阵列后，由于 LED 单元分布位置的不同以及墙面的反射、折射及散射，不可避免地会产生码间干扰，从而降低了系统的性能。自适应均衡技术以及 OFDM 技术也可以降低符号间干扰。目前，应用于 VLC 的均衡和 OFDM 技术的研究已经成为可见光通信研究中的热点。

3. 最后 10 m 距离内的高速接入 VLC 与现有网络的融合接入技术

目前，全球已经开展了光纤到户的工作，并取得了很大的进展。光纤到户后，可为单用户提供 300 Mbps 的下行带宽。在此网络带宽下，目前的微波无线低频段广播覆盖的频谱资源不够，无法满足如此高的带宽需求。因此，在最后 10m 距离内的高速接入将成为宽带通信的瓶颈。可见光波段位于 380～780nm，属于新频谱资源。室内 VLC 由于具有诸多优点，已经成为了理想的短距离高速无线接入方案之一。将可见光通信系统与光纤到户系统融合，可以通过“光电—电光”的转换将信息调制到 LED 光源发射到用户终端，实现高速率、高保密性的无线光接入。此外，如图 6.26 所示，VLC 与 PLC 相融合，可以利用现有的电力线设备传输信号并驱动 LED 光源，将会大幅度降低接入网成本。可以预见，这种技术融合在未来也将会成为可见光通信的研究趋势。

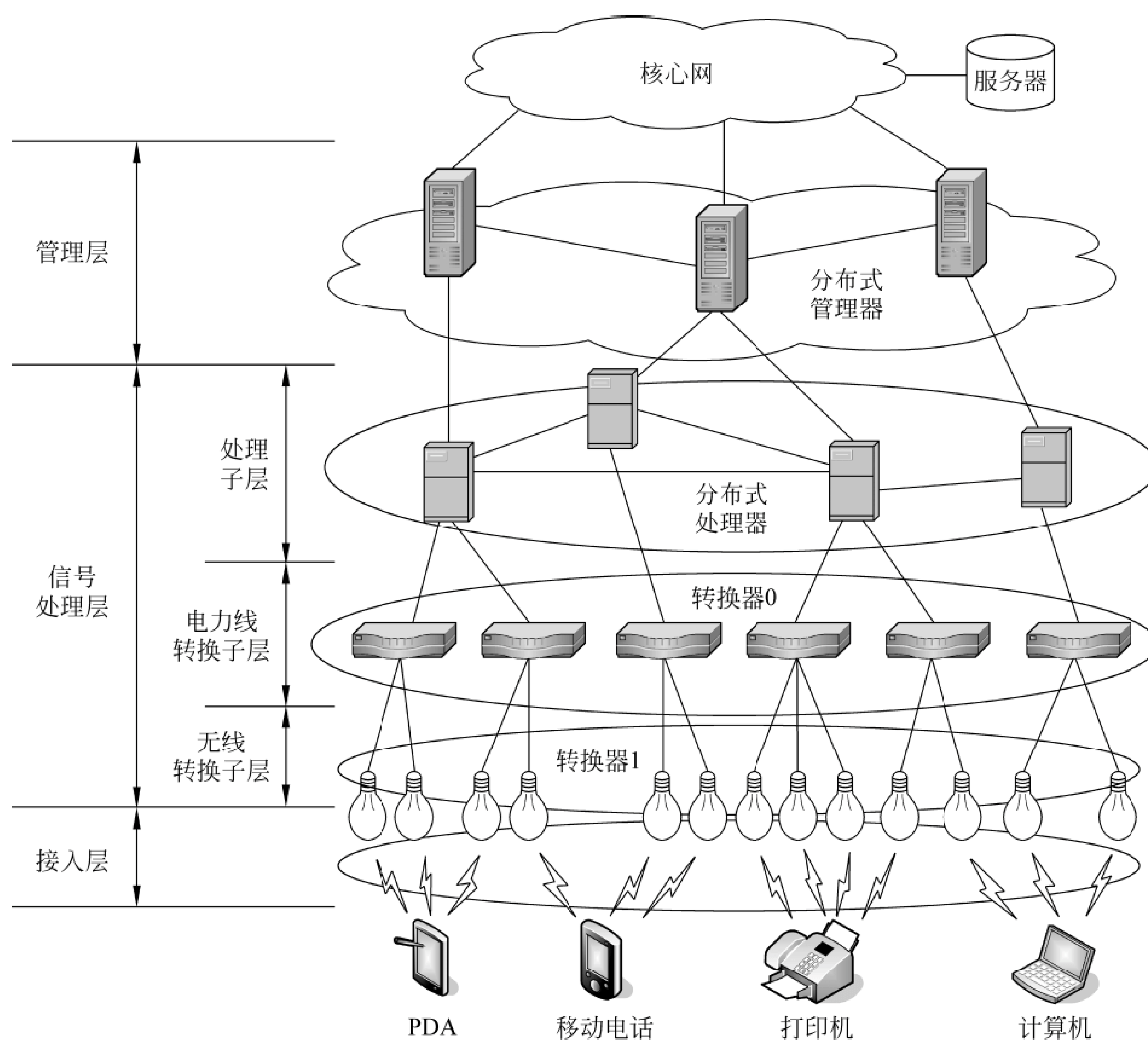


图 6.26　VLC 与 PLC 技术融合的园区网结构

实验 17　用光 MODEM + 无线路由接入

一、实验内容

将局域网用光 Modem + 无线路由方式接入广域网。

二、实验材料和工具准备

（1）光 Modem 一个。

（2）无线路由器一个。

（3）光纤冷接子一对。

（4）光纤若干米。

（5）网线一小段。

（6）光纤冷接工具一套、网线制作工具一套。

三、预备知识

1. 光 Modem

下面以为例加以介绍。

1）接口

光 Modem（光猫）也称为单端口光端机，如图 6.27 所示，它通常带有如下一些接口：



图 6.27　上海贝尔的 1-120 型吉比特无源光纤用户端设备

（1）接口。

- 光口（PON）：SC/PC 单模光纤 GPON 接口。
- PHONE 接口：RJ-11 FXS 接口，用于连接电话机或传真机，提供宽带语音服务。
- LAN2/LAN1：RJ-45 以太网接口，连接固定设备，多作为调试接口。
- POWER：电源接口。

（2）ON/OFF：电源开关。

（3）RESET：复位按钮。

2）指示灯

通常光 Modem 会提供如表 6.8 所示的一些指示灯来指示工作状态。

表 6.8　光 Modem 上的指示灯状态及其含义

指示灯名称	状态	含　义
POWER	绿亮	电源供电正常
	灭	未通电或电源工作不正常
PON	绿亮	光纤链路正常
	闪烁	光纤正在注册
	灭	光 Modem 没有完成与光线路终端（OLT）连接、注册和操作管理
LOS	灭	接收光功率正常
	红闪	接收光功率低于灵敏度要求
INTERNET	绿亮	外网连接成功，但还没有传送数据
	灭	无外网连接
PHONE	绿亮	已经成功注册到软交换
	闪烁	有语音业务流传输
	灭	系统未上电或无法注册到软交换

续表

指示灯名称	状态	含　义
LAN2/LAN1	绿亮	已经与终端设备连接
	闪烁	正在传输数据
	灭	系统未上电或端口未连接网络设备

2. 无线路由器

1）无线路由器的连接

无线路由器是一种 3 层设备，主要用途是与外部网络进行逻辑上的连接。如图 6.28 所示，它可以连接移动/固定终端，以便它们与外网中的设备进行通信。简单地说，它就是给它所连接的终端设备提供一个网络地址。

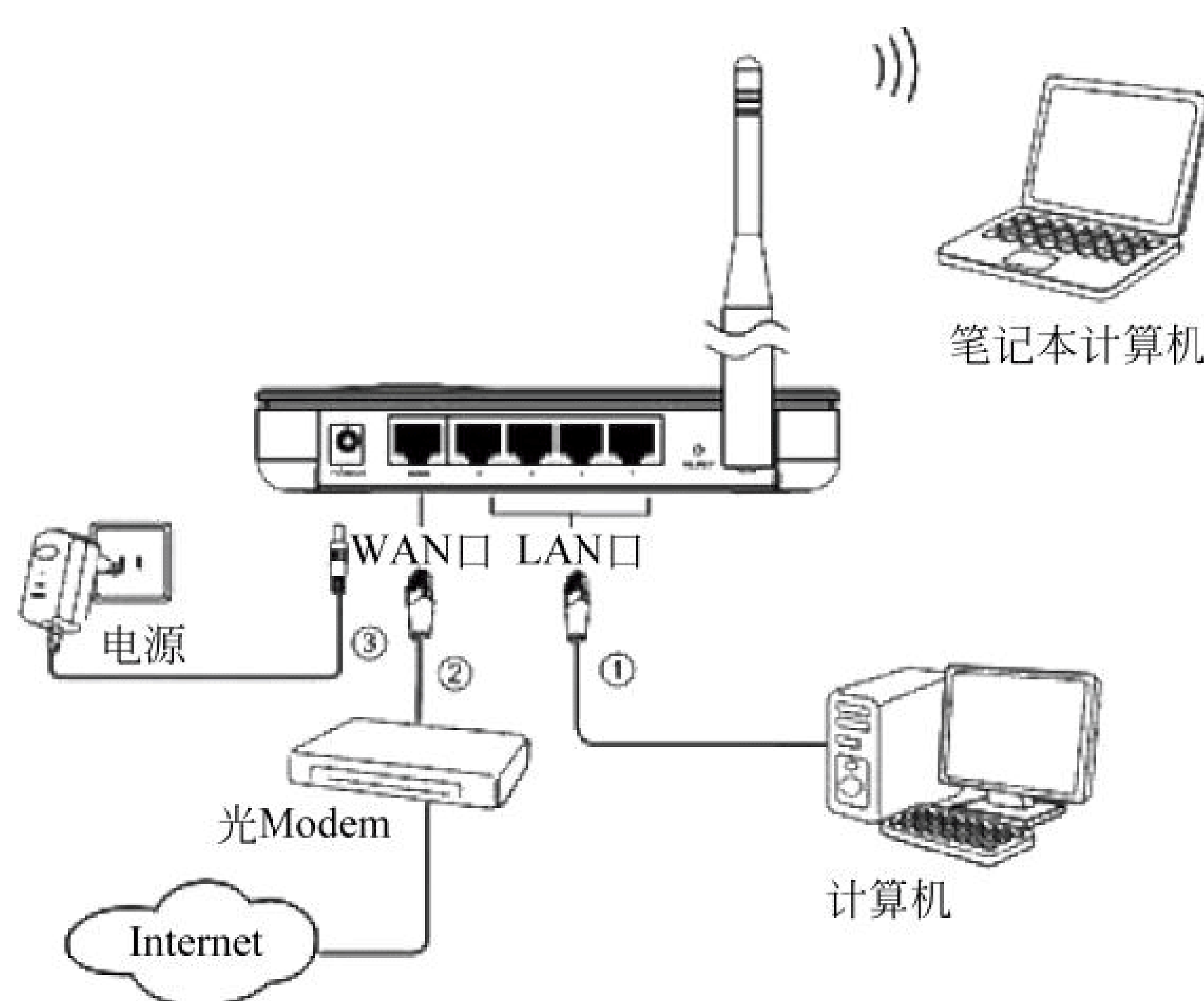


图 6.28　用无线路由器接入 Internet

2）WPS

无线路由的物理连接非常简单，关键在于它的配置。但是，路由器的配置一般比较复杂。一般情况下，用户在新建一个无线网络时，为了保证无线网络的安全，必须在接入点手动设置网络名（SSID）和密钥，然后在客户端验证密钥。这个过程需要用户具备 Wi-Fi 设备的背景知识和修改必要配置的能力。为了减轻客户负担，Wi-Fi 联盟组织实施了一个可选认证项目——WPS（Wi-Fi Protected Setup，Wi-Fi 保护设置），它主要致力于简化无线网络设置及无线网络加密等工作，帮助用户自动设置网络名，配置强大安全增强方案（WPA）及认证功能，并使用户只需输入个人信息码（PIN 方法）或按下按钮（按钮设置，或称 PSC），即可安全连入 WLAN，从而大大简化了无线安全设置操作。但是并非所有 Wi-Fi 认证产品都支持 WPS。

3）上网方式

无线路由器有可能向用户提供 6 种上网方式。

- PPPoE：ADSL 虚拟拨号，需要输入用户名和密码。
- 动态 IP：以太网宽带，自动从网络服务商获取 IP 地址。
- 静态 IP：以太网宽带，使用网络服务商提供的固定 IP 地址。

- L2TP 和 PPTP：基于 VPN（虚拟专用网）的安全上网方式。
- DHCP+：采用 DHCP+认证技术运营商提供的宽带接入服务。

VPN 是通过一个公用网络（Internet）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道，是对内部网的扩展，可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。

4）QSS

QSS 又称快速安全设置，通过按下无线路由和无线网卡上的 QSS 按钮，即可自动建立 WPA2 级别的安全连接，无须在路由器或网卡管理软件的界面上进行烦琐的设置，大大简化了无线安全设置的操作。

四、实验注意事项

（1）勿在雷雨天进行操作。并且在雷雨天将设备电源以及所有连线拆除。

（2）无线路由的位置应尽量放置于：高、平、宽敞处。

五、实验参考步骤

1. 连接光 Modem 到广域网

上电并对照说明书观察有关指示灯是否正常。

2. 连接光 Modem 到无线路由器

连接好后，上电，观察有关指示灯是否正常。通常路由器有 6 种指示灯，指示灯的状态指示了不同的工作状态，如表 6.9 所示。

表 6.9　无线路由器指示灯及其状态指示

符　号	名　　称		状　态		
			常　　亮	闪　　烁	常　　灭
PWR	电源指示灯		已加电	（有的表示 QSS 连接）	未接通电源
SYS	系统状态指示灯		—	工作正常	设备正在初始化
WLAN	无线状态指示灯		—	已经启用无线功能	未启用无线功能
WAN	广域网状态指示灯		端口已连接设备	正在传输数据	端口未连接设备
LAN+标号	局域网状态指示灯		端口已连接设备	端口正在传输数据	端口未连接设备
WPS	安全设定指示灯	绿	安全连接成功	正在安全连接	—
		红	—	安全连接失败	—

注意：

（1）不同的路由器设置的指示灯数目不同，状态指示也有差异，具体请看所带的说明书。

（2）路由器上都会有一个 QSS/RESET 按钮，如图 6.29 所示。它有两个功能：一是 RESET——重启，另一是快速连接无线——有的路由每次开启需要去路由器上按一下 RESET 才能把设备加入到无线网中。

3. 登录配置引导网站

（1）为便于用户配置，商家会给出一个 IP 地址、初始账号和密码。这些都会在商品说明书中给出，或者在路由器底部的标签中标出，并且比较固定，比如 D-Link 无线路由器是 192.168.0.1，TP-Link 路由器是 192.168.1.1；登录账号一般都是 admin，而密码有所不同。

在 LAN 接口中连接一台计算机（笔记本计算机），打开一个浏览器，在地址栏中输入商家给定的那个 IP 地址，单击访问，就会看到如图 6.30 所示的一个无线路由器的设置网页——设置界面。在这个界面中，就可以进行无线路由器相关的设置。下面以 TL-WR941N 型号无线路由器为例，介绍其设置过程。



图 6.29　QSS/RESET 按钮

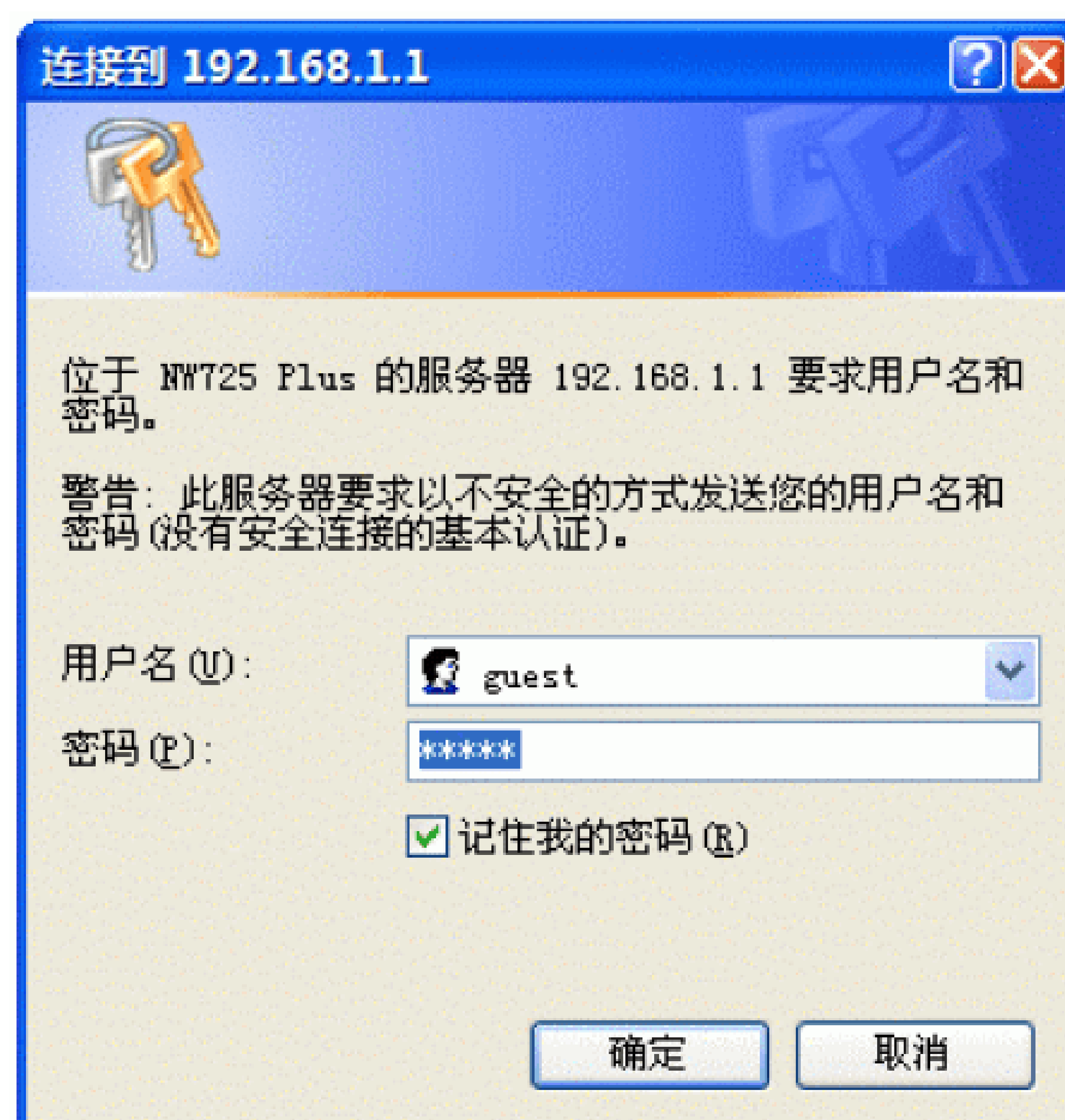


图 6.30　无线路由器的登录界面

（2）登录之后，TP-Link 的设置引导网站首先展示出一个该路由器的“运行状态”界面，如图 6.31 所示。

在如图 6.31 所示的界面中，右侧给出了一些默认的设置数据，左侧提供了多种丰富的设置选项，用户可根据需要对无线路由器进行设置调整。其中有一个向初级用户提供有“设置向导”选项。利用这个选项，就可以简单快捷地搭建无线网络。

4. 使用“设置向导”进行无线设置

① 选择上网方式。单击“设置向导”选项，再单击“下一步”按钮，会出现如图 6.32 所示的“上网方式”界面。

在“设置向导”中，给出了 4 种主要上网方式：PPPoE、动态 IP、静态 IP 和“让路由器自动选择上网方式”。对于初级用户，一般推荐使用智能自动选择上网方式。

② 进行“无线设置”。单击“下一步”按钮，进入“无线设置”界面，如图 6.33 所示。这个界面主要是对无线网络的基本参数以及无线安全进行基本设定。用户可根据实际需求，修改无线网络的状态、SSID、加密设置等。修改 SSID（网络名称），可以方便自己的查找和使用。在“模式”列表框处，建议用户选择混合模式，可以保证对网络设备的最大兼

容性。

• 运行状态
• 设置向导
• QSS安全设置
+ 网络参数
+ 无线设置
+ DHCP服务器
+ 转发规则
+ 安全设置
+ 路由功能
• IP带宽控制
+ IP与MAC绑定
• 动态DNS
+ 系统工具

更多TP-LINK产品，请点击查看 >>

版本信息

当前软件版本： 4.18.29 Build 110909 Rel.35946n
当前硬件版本： WR740N 5.0/6.0 00000000

LAN口状态

MAC 地址： 14-E6-E4-37-3B-50
IP地址： 192.168.1.2
子网掩码： 255.255.255.0

无线状态

无线功能： 启用
SSID号： TP-LINK_373B50
信 道： 自动（当前信道 6）
模 式： 11bgn mixed
频段带宽： 自动
MAC 地址： 14-E6-E4-37-3B-50
WDS状态： 未开启

WAN口状态

MAC 地址： 14-E6-E4-37-3B-51
IP地址： 0.0.0.0 PPPoE自动连接
子网掩码： 0.0.0.0
网关： 0.0.0.0
DNS 服务器： 0.0.0.0 , 0.0.0.0
上网时间： 0 day(s) 00:00:00 正在连接……

WAN口流量统计

	接收	发送
字节数：	0	97355
数据包数：	0	1325

运行时间： 0 天 07:32:20 刷 新

完成

图 6.31　TP-Link 的“运行状态”界面

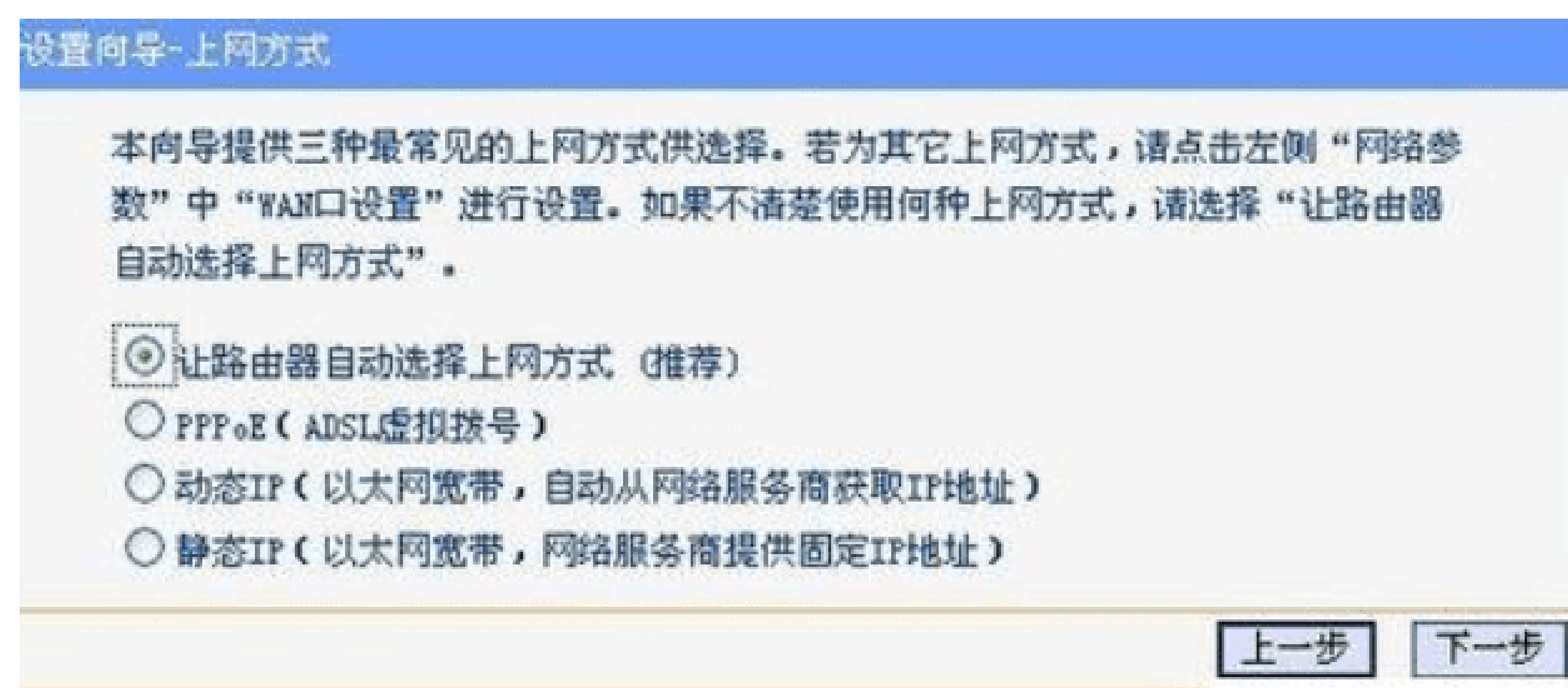


图 6.32　TP-Link 的“上网方式”界面

对于初级用户来说，除在“无线安全选项”中选中 WPA-PSK/WPA2-PSK 单选按钮，并在“PSK 密码”文本框中填入密码外，大多数选项都可以选择默认数据。

图 6.33 “无线设置”界面

③ 单击“下一步”按钮即会看到如图 6.34 所示的“设置完成”的提示，单击“重启”按钮就可完成“设置向导”的设定。随后就会看到如图 6.35 所示的“重新启动”进度条界面。完成后，就会看到如图 6.36 所示的设定好的最终界面。

图 6.34 完成界面

图 6.35 “重新启动”界面



图 6.36　设定好的最终界面

5. *使用功能界面进行无线路由的精准设置*

对于想要进阶的用户，想要发挥无线路由器的功能潜质，就需要在具体的功能界面中进行精准设置。

1）广域网精准设置

选择“网络参数”→“WAN 口设置”命令，弹出如图 6.37 所示的“WAN 口设置”界面。

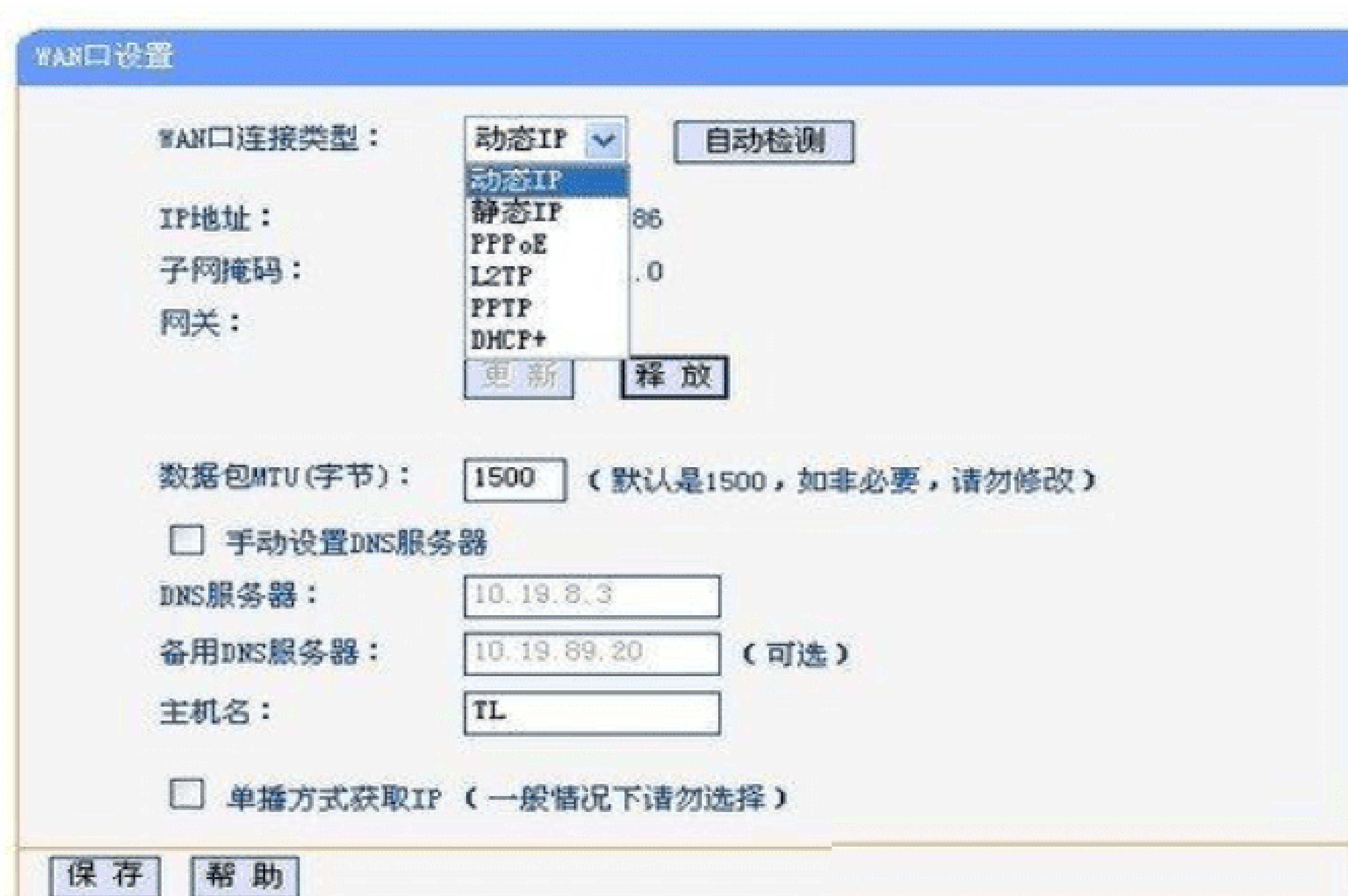


图 6.37　WAN 口（广域网）设置

下面以 WAN 口连接类设置为例介绍广域网精准设计方法。

单击“WAN 口连接类型”中的下拉按钮，可以看到具有 5 种连接类型。与“设置向导”比较，多出了 L2TP、PPTP 和 DHCP+这 3 种模式，提供了更多的选择，用户可以根据运营商提供的网络模式，进行选择。

用户可以单击“自动检测”按钮对网络模式进行智能侦测。

L2TP 和 PPTP 都是基于 VPN(虚拟专用网)的上网方式，是通过一个公用网络（通常指 Internet）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道，是对内部网的扩展，可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。

（1）设置 L2TP 或 PPTP 上网方式。如图 6.38 和图 6.39 所示，需要进行如下操作：

- 账号和口令。可根据 ISP 提供的动态 IP、静态 IP 按需设置 IP，服务器 IP/域名需正确填入 ISP 所提供的 IP 地址或域名。
- 按需选择自动断线等待时间、按需连接、自动连接、手动连接等上网方式。

完成更改后，单击“保存”按钮即可。

图 6.38　常见的 PPPoE 上网方式设置

图 6.39　L2TP 上网方式设置

（2）设置 DHCP+上网方式。如图 6.40 所示，这时也需要正确填入 ISP 提供的上网账号和上网口令，填入认证服务器地址，选择自动或手动连接方式，然后单击“保存”按钮。

图 6.40　DHCP+上网方式设置

通过认证用户的有关信息，确认是合法用户之后，就把相关参数，如 IP 地址、DNS 服务器、子网掩码、网关的地址等传送给用户。用户得到这些参数之后，就能直接进入 Internet 网进行通信，而所有的通信流无须经过 DHCP 服务器。

2）局域网精准设置

在 TP-Link 无线路由器中的“网络参数”里，选择“LAN 口设置”选项，弹出如图 6.41 所示的“LAN 口设置”界面，显示出 3 行数据：MAC 地址、IP 地址和子网掩码。要对局域网进行精确设置，可以通过修改这些数据完成。下面以修改 IP 地址为例，介绍局域网精确设置方法。



图 6.41　局域网（LAN 口）设置

在默认情况下，无线路由器的 IP 地址同上游网关的 IP 地址一致。这样会导致计算机无法获得无线路由器分配的 IP 地址。如果对无线路由器的默认 IP 地址进行修改，就可以防止产生 IP 地址冲突。

如图 6.42 所示，网关地址可以在“WAN 口设置”界面中查到。在“IP 地址”上进行修改，只需与网关的 IP 不同即可。例如，网关的 IP 地址是 192.168.0.1，那么用户就可以将自己的 IP 地址，设置为 192.168.1.1。

改后保存，重启 TP-Link 无线路由器即可。



图 6.42　查询网关地址

3）MAC 地址克隆

MAC 地址克隆是指将无线路由器的广域网(WAN)端口的 MAC 地址，修改为当前计算机网卡的 MAC 地址。这样，ISP 服务器看到的是单台计算机，而实际上是多台计算机在共享上网。

要实现 MAC 地址克隆功能很简单，只需选择“克隆 MAC 地址”，在弹出的如图 6.43 所示的界面中进行克隆即可。保存后重新启动 TP-Link 无线路由器即可正常地多机共享上网冲浪了。

4）无线精准设置

在“无线设置”选项中含有“基本设置”、“无线安全设置”、“无线 MAC 地址过滤”、“无线高级设置”和“主机设置”等子选项。在前面的“设置向导”中，已经进行过无线路

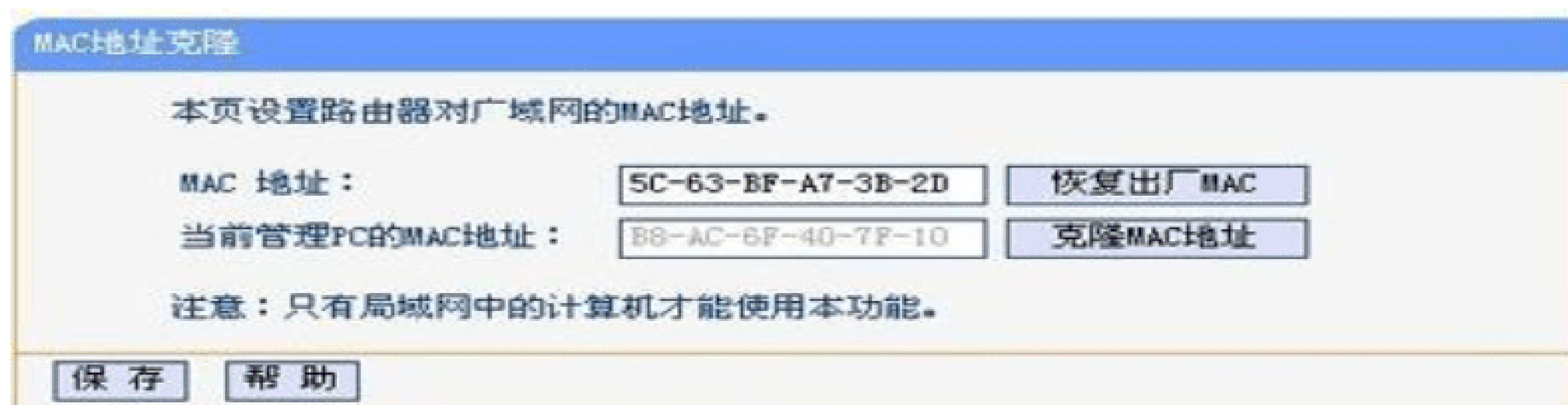


图 6.43　MAC 地址克隆

由器的基本设置，此处不再赘述，仅介绍一点对 TP-Link 无线路由器的“信道”、“频段带宽”或“传输功率”进行调节的方法。

（1）避免“信道”冲突干扰。

众所周知，现在大多数无线设备都使用 2.4GHz 无线频段工作，我国将 Wi-Fi 的该频段分为 13 个信道。可是有很多用户都在使用的无线设备的默认信道“1”，那么当有多个无线设备的信号“相遇”时就会发生冲突和干扰，进而会影响无线传输的质量。

TP-Link 无线路由器支持智能的“自动”信道选择功能。如图 6.44 所示，在“无线网络基本设置”中，将信道采用默认的“自动”，或者挑选一个与周围无线源不同的信道使用，从而避开干扰和冲突，获得最佳无线传输效果。



图 6.44　“信道”冲突干扰的设置

（2）调节“频段带宽”。

频段带宽是发送无线信号频率的标准，频率越高越容易失真，其中 20MHz 在 11n 的情况下能达到 144Mbps 带宽，它穿透性较好，传输距离远（约 100m）；40MHz 在 11n 的情况下能达到 300Mbps 带宽，穿透性稍差，传输距离近（约 50m）。因此，若想获得更大的传输速度，可以选用 40MHz。但在应用环境中，在无线源较多的情况下，任意使用 1～6 信道的无线信号都会干扰 40MHz 频宽的通信，所以不建议选择 40MHz。

如图 6.45 所示，在 TP-Link 无线路由器中可以选择“频段带宽”的“自动”模式，另外，目前大多数无线路由器都支持“20/40MHz 混合”模式，也可以使用。

（3）设定“传输功率”。

传输功率关系到无线路由器的信号表现，因此对于多居室的用户来说，进行无线路由器的无线“传输功率”调节就很有必要。如图 6.46 所示，这款 TP-Link 无线路由器就支持

高、中、低三档的功率调节，用户可根据组网需要进行调整。另外现在大多的无线路由器产品都已支持“传输功率”的调节功能。



图 6.45　调节“频段带宽”



图 6.46　传输功率调整

（4）安全设置。

现在常用的无线加密方式一般分为 3 种：WEP 加密、WPA 加密和 WPA2 加密。WEP 加密较其他加密方式最老，也是最不安全的加密方式。WPA 加密是 WEP 加密的改进版，包含两种方式：预共享密钥和 Radius 密钥。其中预共享密钥（Pre-Share Key 缩写为 PSK）有两种密码方式：TKIP 和 AES，相比 TKIP，AES 具有更好的安全系数，建议用户使用。WPA2 加密，是 WPA 加密的升级版。WPA2 同样也分为 TKIP 和 AES 两种方式。建议选 AES 加密。

如图 6.47 所示，在 TP-Link 无线路由器中，用户可以在“无线安全设置”中进行设置，

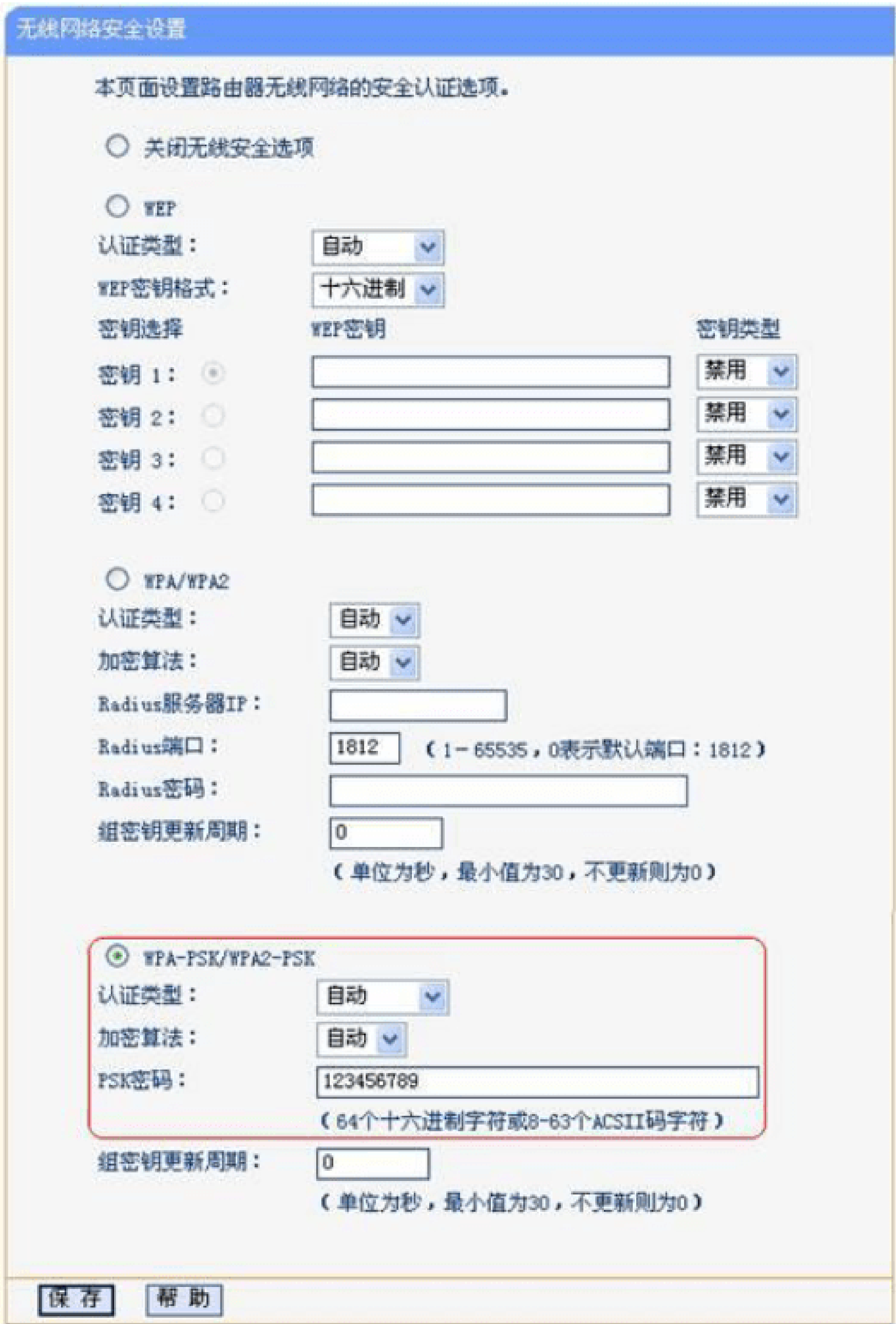


图 6.47　选择 WPA-PSK/WPA2-PSK 加密模式

选择 WPA-PSK/WPA2-PSK 加密模式。然后填入密码，保存和重启即可。

（5）过滤 MAC 地址。

过滤 MAC 地址可以允许某些 MAC 地址通过无线路由访问外部网络，也可以屏蔽某些 MAC 地址访问外部网络。方法如下：

在“无线设置”选项中选择“无线 MAC 地址”过滤子选项，弹出相应的页面，如图 6.48 所示。



图 6.48 “无线 MAC 地址过滤设置”页面

在这个页面中选择“启用过滤层”和过滤规则。过滤规则分为如下两种。

- 禁止：黑名单过滤。
- 允许：白名单过滤。

再单击“添加新条目”按钮，就会进入下一页面，如图 6.49 所示。在这个页面中，可以输入要过滤的地址、状态以及是否生效。添加后，这个条目就会添加到上个页面的下部。例如，刚才添加的张三的 MAC 地址，若前面选择的是“禁止”，则张三所持的 MAC 地址为 00-21-27-B7-7E-15 的设备，就无法通过本路由访问外网了。

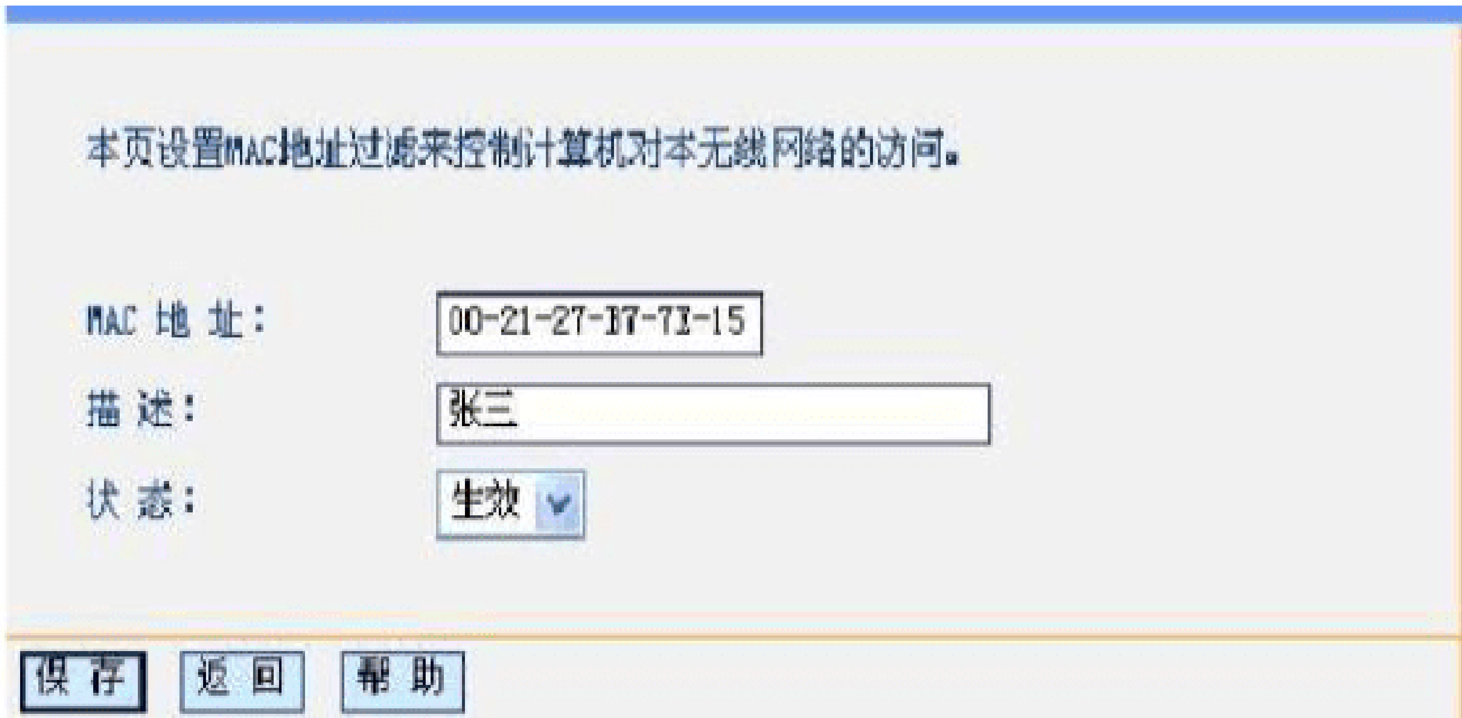


图 6.49 输入过滤地址页面

六、分析与讨论

（1）如果不使用路由器，能上网吗？使用交换机行吗？

（2）没有光纤能上网吗？

习　题　6

一、选择题

1．个人计算机通过电话线拨号方式接入Internet时，应使用的网络设备是【　　】。

A．交换机　　　　B．调制解调器　　　C．浏览器软件　　　D．电话机

2．小明和他的父母因为工作的需要都配备了笔记本电脑，因工作需要他们经常要在家上网，小明家家庭小型局域网的恰当规划是：【　　】。

A．直接申请ISP提供的无线上网服务

B．申请ISP提供的有线上网服务，通过自备的无线路由器实现无线上网

C．家里可能的地方都预设双绞线上网端口

D．设一个房间专门用做上网工作

3．要组建一个有20台计算机联网的电子阅览室，连接这些计算机的恰当方法是【　　】。

A．用双绞线通过交换机连接　　　　B．用双绞线直接将这些机器两两相连

C．用光纤通过交换机相连　　　　　D．用光纤直接将这些机器两两相连

二、填空题

1．ADSL是________传输率的数字传输线技术。

2．________技术是在有线电视台的前端把电视图像用光纤和同轴电缆组合传送给用户。

3．卫星通信系统主要由________和________组成。

三、简答题

1．选择ISP时应考虑哪些因素？

2．*x*DSL包含哪些类型？

3．简述ADSL的工作原理。与其他接入方式相比，ADSL的优势在哪里？

4．试述Cable Modem的工作原理。Cable Modem与普通Modem有何区别？

5．光纤接入有哪些类型？

6．简述卫星通信的特点。

7．简述Wi-Fi的工作原理。

8．简述电力线路接入的基本原理。

9．简述Li-Fi的工作原理。

第 7 章　网 络 安 全

今天，是一个信息时代，也是一个网络时代。网络不仅成为了生活的必需平台，也成为生产必需的平台、学习的必需平台、发展的必需平台。对一个国家，对一个组织，对一个家庭，对一个人，都是这样。其重要性，使其成为谋利者、谋趣者、恶作剧者的攻击目标。于是防御与攻击之间的博弈成为人们必须特别关注的领域。但是，保障互联网的安全是极为复杂而困难的。这是因为：

（1）网络是一种重要的系统，重要的系统往往是攻击的目标。

（2）网络是一个复杂的系统，而复杂的系统往往是脆弱的。

（3）互联网是一个开放的系统，开放的系统方便了应用，也方便了攻击。

（4）攻击与防御本身是不对称的：

- 攻击可以在某个时刻进行，而防御必须全天候进行，因为防御不知道攻击在什么时刻发起。
- 攻击可以在某个点上进行，而防御必须全方位布局，因为防御不知道攻击选在什么点上。
- 攻击可以采用某一种技术，而防御必须考虑所有可能，因为防御不知道攻击用了什么技术。

困难是有志者的动力，它激发了有志者们攻克困难的激情。

7.1　网 络 入 侵

网络入侵主要有两种形式：恶意程序入侵和黑客入侵。

7.1.1　恶意程序入侵

1．恶意程序的概念

恶意程序是一类可以危害系统或应用正常功能的特殊程序或程序片段。恶意程序的表现多种多样，因恶意程序制造者的兴趣和目的而异，例如：

- 修改合法程序，使之变为有破坏能力的程序；
- 利用合法程序，非法获取或篡改系统资源或敏感数据。

2．恶意程序的类型

恶意程序名目繁多，并且还在通过改进、混合、技术交叉等手段，生成新的品种。下面仅介绍几种常见的恶意程序。

1）陷门

陷门（trap doors）是为程序开辟的秘密入口。本来陷门是程序员们进行程序测试与调试而编写的程序片段，但也发展成为攻击者们的一种攻击手段。

- 利用陷门进行远程文件操作和注册表操作；
- 利用陷门记录各种口令，获取系统信息或限制系统功能。

2）逻辑炸弹

逻辑炸弹是嵌入在某个合法程序中的一段程序，它在某种条件下会被“引爆”，产生有害行为，如改变、删除数据或整个文件，执行关机操作，甚至破坏系统。

3）特洛伊木马

特洛伊木马的名字来自古代的一次战争。在这次战争中，希腊人在一个名叫特洛伊（今天的土耳其境内）的城外丢弃了一种木制的马，它看起来好像是在企求和平，马肚子里却藏着几十位战士。后人常把看起来有用或无辜，实际却有害的东西称为特洛伊木马。

特洛伊木马程序就是一些看起来有用，但也包含了一段隐藏的、激活时将执行某些破坏性功能的代码。

4）蠕虫

网络蠕虫是一种可以独立运行的恶意程序，它可以通过网络（永久性网络连接或拨号网络），并在网络中爬行的过程中进行繁衍。通过自身大量繁衍，消耗系统资源，甚至导致系统崩溃；并且它还可以携带别的恶意程序，对系统进行破坏活动。

为了自身复制，网络蠕虫使用了一些网络传输机制，如电子邮件机制（通过电子邮件进行传播）、远程执行机制（执行自身在另一个系统中的副本）、远程注册机制（注册到另一个远程计算机中进行繁衍）等。典型的网络蠕虫只会在内存中维持一个活动副本，并不向磁盘中写任何东西。

5）流氓软件

流氓软件最早出现于 2001 年，其发展大致经历了恶意网页代码、插件推广、软件捆绑和流氓软件病毒化 4 个阶段。

恶意网页代码是某些黄色网站和中小网站提高网站访问量的重要手段。它们在其网站页面中放置一段恶意代码，当用户浏览这些网站时，用户的 IE 浏览器主页会被修改为当前网页。甚至通过恶意网页代码可以直接对用户计算机的注册表进行修改，对一些系统功能进行限制，如禁用 IE 设置、注册表编辑器、DoS 等。

插件推广技术随着 2003 年出现的“中文上网”业务诞生。“中文上网”的作用是将中文解析成对应的网址，使用户输入中文的公司或网站名称时能够打开它们的网站，而要想实现这个功能，就需要在用户计算机上安装一个插件程序。为提升其品牌价值，“中文上网”业务公司与大量的网站进行合作，放置其插件程序，使得用户访问这些网站时被自动安装上“中文上网”插件，并且无法卸载。

软件捆绑是互联网厂商向用户的计算机中安插流氓软件的另一条重要途径。这些厂商网罗了多种知名共享软件的作者，将自身的产品与共享软件捆绑，并支付一定费用。当用户安装这些共享软件时，会同时被强制安装流氓软件，且无法卸载。2006 年下半年，大量的“流氓软件”开始使用计算机病毒隐藏自身，进行快速传播，并对抗用户的清除。

随着流氓软件的肆虐，流氓软件的检测和清除卸载工具也纷纷涌现，典型的有瑞星的“卡卡上网助手”、流氓软件清理助手、Windows 流氓软件清理大师、金山系统清理专家等。

6）病毒

“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或程序代码。”（1994 年 2 月 28 日颁布的《中华人民共和国计算机信息系统安全保护条例》）。通常认为，计算机病毒具有如下基本特点。

- 隐蔽性：巧妙地隐藏，使得难于发现，通常还具有变异性和反跟踪能力。
- 传染性：主要的两种传染途径是引导扇区传染和文件传染。
- 潜伏性（触发性）：在一定的条件下才发作，目的不易被发现。
- 破坏性：如修改数据、消耗系统资源、破坏文件系统等。

从上面的讨论可以看出，病毒只是恶意程序中的一种，它与其他恶意程序还是有一定的不同的。但是，它们的共同之处都是会对系统造成危害。同时，由于现在的恶意程序已经不是单一的技术，大都采用了两种以上技术，使得恶意程序间的界限变得模糊，形成各种改良型、混合型、交叉型和多态型的恶意程序。人们也不再刻意去对它们进行分类，一般统称为病毒。

3. 网络病毒防范

目前，计算机网络主要采用 C/S 工作方式，其最主要的软、硬件实体是工作站和服务器，病毒在网络中是通过“工作站—服务器—工作站”的方式传播的。因此，基本的病毒预防主要应当从工作站和服务器两个方面进行。

1）基于工作站的防病毒技术

工作站是网络的门户，把好了门户，才能有效地防止病毒的入侵。工作站上的防病毒技术主要有使用防毒杀毒软件、安装个人防火墙、使用无盘工作站和备份。

2）基于服务器的防病毒技术

基于服务器的防病毒技术主要是提供实时病毒扫描能力，全天候地对网络中的病毒入侵进行实时检测。主要方法有实时在线病毒扫描、服务器扫描和工作站扫描。

7.1.2 黑客入侵

1. 黑客进行远程攻击的一般过程

（1）收集被攻击目标的有关信息，分析这些信息，找出被攻击系统的漏洞。

黑客确定了攻击目标后，一般要收集被攻击者的信息，包括目标机的类型、IP 地址、所在网络的类型、操作系统的类型、版本、系统管理人员的名字、邮件地址等。

对攻击对象信息的分析，可找到被攻击系统的漏洞。例如，运行一个 Host 命令，可以获得被攻击目标机的 IP 地址信息，还可以识别出目标机操作系统的类型；利用 Whois 查询，可以了解技术管理人员的名字；运行一些 Usernet 和 Web 查询，可以了解有关技术人员是否经常上 Usernet 等；一个管理人员经常讨论的问题也可以表明其技术水平的高低等。通过这些，就可以找到对方系统的漏洞。

（2）用适当工具进行扫描。在对操作系统进行分析的基础上，黑客常编写或收集适当的工具，在较短的时间内对目标系统进行扫描，进一步确定攻击对象的漏洞。

（3）建立模拟环境，进行模拟攻击，测试对方反应，找出毁灭入侵证据的方法。

（4）实施攻击。

2．黑客的常用工具

随着计算机技术的进步，黑客技术也在迅速发展，出现了专业化的黑客工具。据统计，目前黑客可以使用的攻击软件已达千种以上。

1）扫描器

扫描器是自动检测远程或本地主机安全性弱点的程序。它不仅是黑客们的作案工具，也是管理人员维护网络安全的有力工具。常用的扫描器很多，如网络安全扫描器 NSS、超级优化 TCP 端口检测程序 Strobe、安全管理员网络分析工具 SATAN 等。

2）口令入侵工具

口令入侵是指破解口令或屏蔽口令保护。由于真正的加密口令是很难逆向破解的，黑客们常用的口令入侵工具所采用的技术是仿真对比，利用与原口令程序相同的方法，通过对比分析，用不同的加密口令去匹配原口令。

3）特洛伊木马（Trojan horse）

特洛伊程序可以提供或隐藏一些功能，这些功能可以泄露系统的一些私有信息或控制该系统。

4）网络嗅觉器（sniffer）

Sniffer 可以使网络接口处于广播状态，从而为截获信息带来便利。由于它在网络上不留下任何痕迹，所以不易被发现。

5）系统破坏装置

常见的系统破坏装置有邮件炸弹和病毒。邮件炸弹是指不停地将无用信息传送给攻击对象，填满其信箱，使其无法接收有用信息。

3．漏洞扫描

漏洞扫描就是自动检测计算机网络系统在安全方面存在的可能被黑客利用的脆弱点。漏洞扫描技术通过安全扫描程序实现。所谓扫描，包含了非破坏性原则，即不对网络造成任何破坏。在实施策略上可以采用被动式和主动式两种策略。

1）被动式扫描策略

被动式扫描策略主要检测系统中不合适的设置、脆弱的口令以及同安全规则相抵触的对象。

2）主动式扫描策略

主动式扫描策略是基于网络的扫描技术，主要通过一些脚本文件对系统进行攻击，记录系统的反应，从中发现漏洞。

目前，扫描程序已经发展到了几十种，有的小巧快捷，有的界面友好；有的功能单一，有的功能完善。被广泛使用的扫描程序有 NSS、Strobe、SATAN、Ballista、Jakal、IdentTCPscan、

Ogre、WebTrends、Security、Scanner、CONNECT、FSPScan、XSCAN、ISS、“火眼”等。

4. IP 欺骗

简单地说，IP 欺骗的基本思路是：假定要攻击主机 X，首先要找一个 X 信任的主机 A，攻击者（主机 B）假冒 A 的 IP 地址（对 IP 堆栈中的地址进行修改），建立与 X 的 TCP 连接，并对 X 进行攻击。

7.2 数据加密与数字签名

网络安全的核心是数据资源的保护。数据保护主要涉及如下 3 个方面。

- 机密性（confidentiality）保护：不为非授权获取者理解和使用。
- 完整性（integrity）：使数据在传输、存储过程中不受到未授权的篡改和破坏。
- 抗抵赖性（non-repudiation）：防止输出发送者或接收者事后对自己行为的否认。

数据的意义在于其所包含的信息。加密是一种数据屏蔽，其基本思想是将数据变形，使非法获取者无法辨别其所包含的信息内容、无法利用。

7.2.1 加密/解密算法和密钥

数据加密是通过某种函数进行变换，把直接可读数据报文（称为明文或明码）转换为不可直接阅读的密文（也称密码），可以描述为

$$C=E_k(M)$$

其中，k 为密钥，M 为明文，C 为密文，E 为加密算法。

为了进行加密变换，需要密钥和算法两个要素。进行解密，也需要这两个要素。在这里可以粗略地看到，为了提高加密强度，一是要设计安全性好的加密算法，二是要尽量提高密钥的长度（因为利用现代计算机技术可以用穷举法，穷举出密钥，加长密钥可以增加穷举的时间）。

除此之外，人们还考虑，如果能找到一对不同的密钥，用一个加密，用另一个解密，则密码系统的强度就会大大提高。于是，就出现了两种密码体系：对称密码体系和不对称密码体系。前者加密与解密用同一把密钥，后者加密与解密用不同的密钥。不对称密钥体系虽然加密强度高，但效率较低。

7.2.2 对称密钥体系

如图 7.1 所示，在对称型密钥体系中，加密和解密采用同一密钥（或者说，很容易相互导出）。由于加解密采用同一密钥，密钥绝不能泄露，故也将这种体系称为秘密密钥密码体

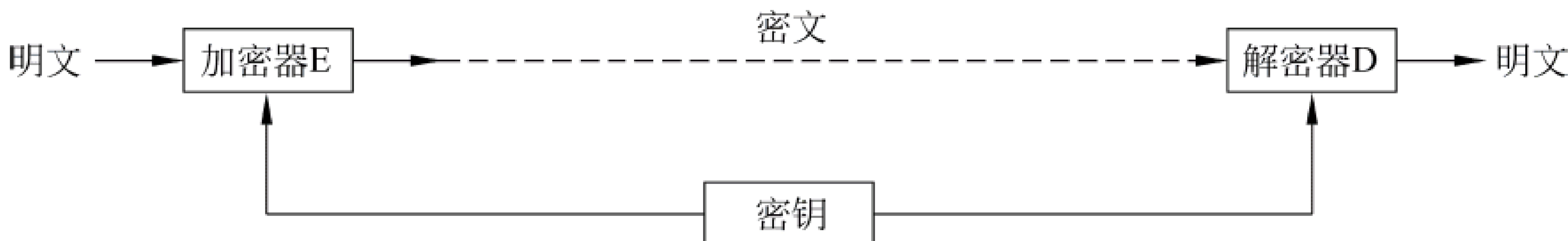


图 7.1　对称密钥体制的加密与解密

制或私钥密码体制。

在对称密码体系中，最著名的加密算法是 IBM 公司于 1971—1972 年间研制成功的数据加密标准（Data Encryption Standard，DES）分组算法，1977 年被定为美国联邦信息标准。DES 使用 64 位的密钥（除去 8 位奇偶校验码，实际密钥长度为 56 位），对 64 位二进制数进行分组加密，经过 16 轮的迭代、乘积变换、压缩变换等处理，产生 64 位密文数据。

IDEA（International Data Encryption Algorithm）是于 1992 年推出的另一个成功的分组加密算法。它的核心是一个乘法/加法非线性构件，通过 8 轮迭代，能使明码数据更好地扩散和混淆。

加密密钥系统运算效率高、使用方便、加密效率高，是传统企业中最广泛使用的加密技术。但是，由于秘密密钥要求通信的双方使用同样的密钥，导致了对称密钥加密系统存在两个难以克服的问题。

1）密钥的管理和分配问题

密钥的管理和分配问题是指：由于通信双方在通信之前必须互通密钥，而密钥在传递的过程中极有可能被第三方截获，这就为密钥的保密工作增加了难度；另外，如果有 n 个用户彼此之间要进行保密通信，则一共需要 n（n−1）/2 个密钥，如此巨大数目的密钥为密钥的管理和分配带来了极大的困难。

2）认证问题

所谓认证问题，是指对称密钥加密系统无法避免和杜绝如下一些不正常现象：

- 接收方可以篡改原始信息；
- 发送方可以否认曾发送过信息等。

7.2.3 非对称密钥体系

针对私钥加密系统的缺点，1976 年 Diffie 和 Hellman 提出了非对称密钥系统。非对称加密技术使用两把不同的密钥：私钥和公钥，从一个很难推出另一个。发送方使用对方的公钥加密，接收方使用自己的私钥解密，即公钥公开，私钥保密。因此，非对称密钥系统又称为公开密钥系统。

公开密钥系统的主要优点是发送者和接收者事先不必交换密钥，从而使保密性更强。另外，公开密钥系统还可用于身份认证和防止抵赖，这在保密通信中被称为数字签名，它在现在和将来的电子商务活动中具有远大的应用前景。

7.2.4 数字签名

数据加密的主要目的是防止第三方获得真实数据。但是，这并没有解决通信双方有可能由于社会原因引起的纠纷。

- 否认：发送者事后不承认已发送过的信息，或接收者事后不承认接收过的信息；
- 伪造：接收者伪造一份来自发送者的信息；
- 篡改：接收者私自修改接收到的信息；
- 冒充：网络中某一用户冒充发送者或接收者。

数字签名（digital signature）是一种信息认证技术，它利用数据加密技术、数据变换技

术，根据某种协议来产生能反映被签署文件和签署人的特征，以保证文件的真实性和有效性，同时也可用来核实接收者是否有伪造、篡改行为。

将数字签名和公开密钥相结合，可以提供安全的通信服务。其要点在于发送方不是简单地将明文和签名发送出去，而是先用接收方的公开密钥进行加密后再发送出去。接收方收到被加密的报文后，先用自己的私有密钥进行解密后，再进行数字签名比较。

7.2.5 数字证书与 PKI

1．概述

任何密码体制都不是坚不可摧的，公开密钥系统也不例外。由于公开密钥系统的公钥是对所有人公开的，从而免去了密钥的传递，简化了密钥的管理。但是，这个公开性在给人们带来便利的同时，也给攻击者冒充身份以有机可乘，造成公钥体系中的公钥被篡改问题（public key tampering）。例如，若用户甲要和用户乙通信，那么甲必须要有乙的公钥，假设甲从 BBS 上下载了乙的公钥，并用它加密信件，然后发给了乙。但是，遗憾的是，甲和乙都不知道，丙在这之前已潜入了 BBS，并用自己生成的公钥替换了乙的公钥。事实上，甲用来发信的公钥已不是乙的公钥而是丙的公钥。于是，丙就可以用他手中的私钥来解密甲以及所有用户给乙的信，也还可以用乙真正的公钥来转发其他用户给乙的信，而用户甲和用户乙全然不知。

容易看出，造成以上诸多问题的最根本原因是用户甲拿到的用户乙的公钥是一个假的密钥。也就是说，密钥也需要认证，在拿到某人的公钥时，需要先辨别一下它的真伪。在日常生活中，辨别一个人的身份是查看它的身份证、工作证等证件。在计算机网络中也是一样，可以通过查看一个公钥的公钥证书来辨别其真伪。而公钥证书就像身份证、工作证一样是由权威机构颁发的。颁发公钥证书的机构称为认证机构体系（Certificate Authority，CA），它一般由大家都信任的权威机构如政府部门或金融机构来充当，负责发放和管理电子证书，使网上通信的各方能互相确认身份。

2．CA 的主要职责

CA 的主要职责如下。

- 颁发证书：如密钥对的生成、私钥的保护等，并保证证书持有者应有不同的密钥对。
- 管理证书：记录所有颁发过的证书，以及所有被吊销的证书。
- 用户管理：对于每一个新提交的申请，都要和列表中现存的标识名相比照，如出现重复，就予以拒绝。
- 吊销证书：在证书有效期内使其无效，并发表 CRL（被吊销的证书列表）。
- 验证申请者身份：对每一个申请者进行必要的身份认证。
- 保护证书服务器：证书服务器必须是安全的，CA 应采取相应措施保证其安全性。例如，加强对系统管理员的管理、防火墙保护等。
- 保护 CA 私钥和用户私钥：CA 签发证书所用的私钥要受到严格的保护，不能被毁坏，也不能非法使用。同时，要根据用户密钥对的产生方式，CA 在某些情况下有

保护用户私钥的责任。

- 审计与日志检查：为了安全起见，CA 对一些重要的操作应记入系统日志。在 CA 发生事故后，要根据系统日志做善后追踪处理——审计。CA 管理员要定期检查日志文件，尽早发现可能的隐患。

3．PKI

PKI（Public Key Infrastructure，公开密钥基础设施）是一种基于公开密钥理论的网络安全平台和信任体系。它采用证书管理公钥，通过第三方的可信机构 CA，把用户的公钥和用户的其他标识信息（如名称、E-mail、身份证号等）捆绑在一起，在 Internet 上验证用户的身份。一个典型、完整、有效的 PKI 应用系统至少应具有以下功能：

- 公钥密码证书管理；
- 黑名单的发布和管理；
- 密钥的备份和恢复；
- 自动更新密钥；
- 自动管理历史密钥；
- 支持交叉认证。

如图 7.2 所示，典型的 PKI 包含如下 5 个部分。

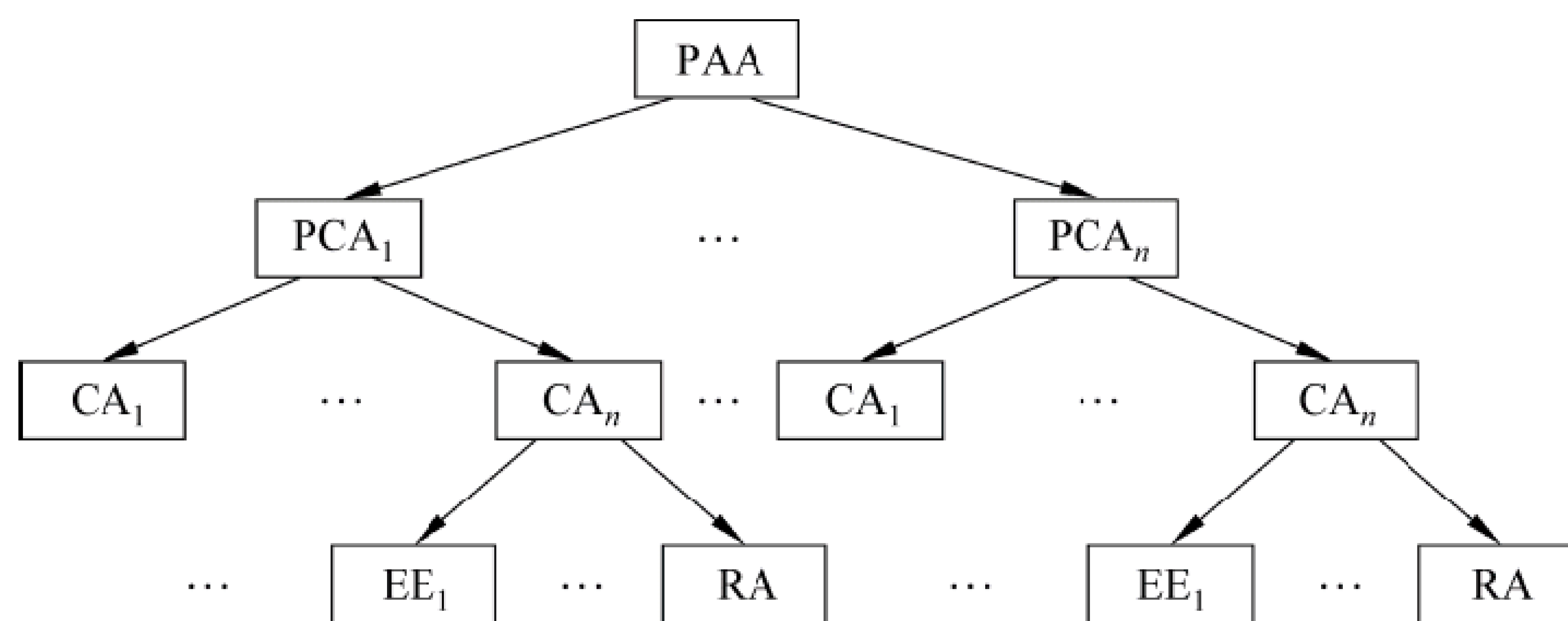


图 7.2　典型的 PKI 结构

（1）政策批准机构 PAA。PAA 是一个 PKI 系统方针的制定者，具有如下功能：

- 建立整个 PKI 体系的安全策略；
- 批准本 PAA 下属的 PCA 的政策；
- 为下属 PCA 签发证书；
- 负有监控各 PCA 行为的责任。

（2）政策 CA 机构 PCA。制定本 PCA 的具体政策。

（3）注册中心（Registration Authority，RA）。RA 根据 PKI 的管理政策，核实证书申请者的身份，负责证书的审批。

（4）认证中心（CA）。CA 是被信任的部门，负责证书的颁发和管理，它使用自己的私钥对 RA 提交的证书申请进行签发，以保证证书数据的完整性。一个 PKI 系统往往包含了许多 CA。这些 CA 按照层次结构进行管理，使各 CA 之间可以交叉认证，形成一个 PKI 的信任模型。

有些 PKI 系统的 CA 包含了 RA 的功能。

（5）证书库（repository）。证书库存放了 CA 已经签发的证书和已经撤销的证书，并且通过目录服务提供网络服务。

（6）用户（client）。用户有两类：证书的持有者（certificate holder）和证书的信任者。

由于 PKI 体系结构是目前比较成熟、完善的 Internet 网络安全解决方案，国外的一些大的网络安全公司纷纷推出一系列的基于 PKI 的网络安全产品，如美国的 Versign、IBM、Entrust 等安全产品供应商为用户提供了一系列的客户端和服务器端的安全产品，为电子商务、政府办公网、EDI 等提供了完整的网络安全解决方案。

7.3 身 份 识 别

在计算机网络中，身份认证就是鉴别系统资源使用者的身份是否合法，或者在通信时对方的身份是否可以认可。通常，用户或系统可以使用下列方法来证明自己的身份。

7.3.1 静态口令

口令通常是作为用户账号补充部分向系统提交的身份凭证。一般说来，用户账号是公开的。当用户向系统提交了账号以后，还需要提交保密形式的凭证——口令，供系统鉴别用户的真实性，以防止非法使用用户账号的登录。所以，用户只有向系统输入口令后，通过了系统的验证，才能获得相应的权限。

口令一旦失密或破解，该用户的账号就不再受到保护，攻击者就可以大摇大摆地进入系统。因此，口令的保护是用户和系统管理员都必须重视的工作。下面从几个方面考虑口令的安全。

1．基于口令本身的安全保护

（1）扩大口令的字符空间。口令字符空间越大，穷举攻击的难度就越大。一般地，不要仅限于使用 26 个大写字母，可以扩大到小写字母、数字等计算机可以接受的字符空间。

（2）选择长口令。口令越长，破解需要的时间就越长，一般应使位数大于 6 位。

（3）使用随机产生的口令，避免使用弱口令（有规律的口令）和容易被猜测的口令，例如家庭成员或朋友的名字、生日、球队名称、城市名等。

（4）使用多个口令，在不同的地方不要使用相同的口令。

（5）缩短口令的有效期。口令要经常更换。最好使用动态的一次性口令。

2．基于验证过程的口令安全保护

（1）限制口令的验证次数。

（2）限制登录时间，如属于工作关系的登录，把登录时间限制在上班时间内。

（3）增加口令认证的信息量。例如在认证过程中，随机地提问一些与该用户有关，并且只有该用户才能回答的问题。

（4）使用软键盘输入口令。软键盘是一种显示在屏幕上的键盘，可供用户用鼠标选择点击进行输入。如图 7.3 所示，软键盘上的键的布局可以是随机的，这样就能有效地防止木

马通过对按键位置的记录，窃取用户密码。



图 7.3　某银行的客户端登录软键盘

（5）用验证码防止批量登录攻击。验证码也称 CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart，全自动区分计算机和人类的图灵测试），是一种区分用户是计算机和人的公共全自动技术，其目的是有效防止某一个特定注册用户用特定程序暴力破解方式进行不断的登录尝试。其具体方法是强迫用户在登录时，必须要人工进行一些工作。基本方法是要用户从模糊的图形之中，辨认出隐藏在其中的一些信息。用户只有将正确的答案与账户和口令一起发送，才能注册。这就使得攻击者使用程序自动注册成为不可能。

在形式上，验证码可以是数字、字母、文字、图片、广告以及问题等。图 7.4 为不同形式的验证码示例。

验证码主要用来控制注册或登录的时间和节奏不能太快。用户登录时，验证码根据时间周期随机生成，用户在一定的时间周期内必须从图片中人工找出所隐藏的信息输入验证码，提交服务器系统验证，验证成功才能登录。两次登录之间有一个验证生存期（一般为 30s）。

强制人为干预的另一种方法是，通过手机传送验证码。

3．基于保存与管理的指令安全

（1）口令的存储不仅是为了备忘，更重要的是系统要在检测用户口令时进行比对。直接明文存储口令（写在纸上或直接明文存储在文件或数据库中）最容易泄密。较好的方法是将每一个用户的系统存储账号和杂凑值存储在一个口令文件中。当用户登录时，输入口令后，系统计算口令的杂凑码，并与口令文件中的杂凑值比对：成功，则允许登录；否则，拒绝。

（2）系统管理员除对用户账户要按照资费等加以控制外，还要对口令的使用在以下几个方面进行审计：

- 最小口令长度；
- 强制修改口令的时间间隔；
- 口令的唯一性；
- 口令过期失效后允许入网的宽限次数；如果在规定的次数内输入不了正确口令，则认为是非法用户的入侵，应给出报警信息。



图 7.4　几种不同风格的验证码

7.3.2　动态口令

1. 动态口令的概念

动态口令也称一次性口令（One-Time Password，OTP），是最安全的口令。它是根据专门的算法生成一个不可预测的随机数字组合，每个密码只能使用一次，目前被广泛运用在网银、网游、电信运营商、电子商务、企业等应用领域。

动态口令有如下优势：

- 可以提供最终用户安全访问企业核心信息的手段。
- 可以降低与密码相关的 IT 管理费用。
- 是一种无须记忆的复杂密码，降低了遗忘密码的几率。

2. 动态令牌的类型

为了安全，动态口令不是在网络上直接生成，也不是有系统直接从网络上发给用户，而是通过其他渠道或生成器提供给用户。这些用于生成动态口令的终端通常称为“令牌”。目前主流令牌有短信密码、手机令牌、硬件令牌、软件令牌 4 种。

1）短信密码

短信密码以手机短信形式请求包含 6 位或更多随机数的动态口令，身份认证系统以短

信形式发送随机的 6/8 位密码到客户的手机上，客户在登录或者交易认证时候输入此动态口令，从而确保系统身份认证的安全性。

2）手机令牌

手机令牌是一种手机客户端软件，它每隔 30s 产生一个随机 6 位动态密码，口令生成过程不产生通信及费用，具有使用简单、安全性高、低成本、无须携带额外设备、容易获取、无物流等优势，手机令牌是 3G 时代动态密码身份认证发展趋势。手机令牌有 J2ME、iPhone、Andriod、Windows Mobile 6 版本，可以广泛应用在网络游戏、互联网等用户基数大的领域，手机令牌的使用将大大减小动态密码服务管理及运营成本，方便用户。

3）硬件令牌

硬件令牌往往是一个钥匙扣大小的轻巧器具，上有显示屏可以显示随机密码。它每 60s 变换一次动态口令，动态口令一次有效，它产生 6/8 位动态数字。图 7.5 是一款硬件令牌。



图 7.5　一款硬件令牌

4）软件令牌

软件令牌是通过软件生成随机密码。

3. 动态口令技术分类

动态口令技术主要分两种：同步口令技术和异步口令技术（挑战-应答方式）。其中的同步口令技术又分为时间同步口令和事件同步口令两种。

1）时间同步口令

时间同步口令基于令牌和服务器的时间同步，并且采用国际标准时间，一般每 60s 产生一个新口令。为了保持服务器与令牌的同步，一方面要求服务器要能够十分精确地保持正确的时钟，对令牌的晶振频率也有严格的要求；另一方面由于令牌的工作环境不同，在磁场、高温、高压、震荡、浸水等情况下易发生时钟脉冲的不确定偏移和损坏，因此在每次进行认证时，服务器端将会检测令牌的时钟偏移量，不断微调自己的时间记录。

2）事件同步口令

基于事件同步的令牌是通过某一特定的事件次序及相同的种子值作为输入，通过 HASH 算法运算出一致的密码。其整个工作流程同时钟无关，不受时钟的影响，令牌中不存在时间脉冲晶振。但由于算法的一致性，其口令是预先可知的，通过令牌，可以预先知道今后的多个密码，故当令牌遗失且没有使用 PIN 码对令牌进行保护时，存在非法登录的风险。因此对于 PIN 码的保护是十分必要的。

3）异步口令

异步口令不需要令牌和服务器之间同步，因而降低了对应用的影响，极大地提高了系统的可靠性。它的主要技术是采用了挑战/应答（challenge-response）方式。

基于挑战/应答方式的身份认证系统在是每次认证时，认证服务器端都给客户端发送一个不同的“挑战”字串，客户端程序收到这个“挑战”字串后，做出相应的“应答”，具体过程已经在 6.1.3 节介绍。

7.3.3 基于密钥分发的身份认证

简单地说，认证协议主要有两种作用：提供机密性和认证性。密钥是加密的工具，其私密性，使它也具有了凭证的某些特性。在网络环境下，密钥分发是通过握手过程进行的，这个过程要遵守某种规则，这些称为认真协议或算法。在这个过程中也有了身份认证的作用。需要注意的是，“身份”不仅包含了真实性，还包括了时效性，即此刻的 A，不是彼刻的 A，只有确认了这一点，才能有效地防止抵赖行为。

基于密钥分发的身份认证方法很多，按照认证方向可以分为单向认证和双向认证；按照需不需要可信的第三方介入，可以分为基于密钥的直接身份认证和基于密钥的间接身份认证。这里，可信的第三方多是由 KDC（Key Distribution Center，Key Distribution Center，密钥分发中心）担当。下面介绍几种常用的身份认证协议。

1. 基于公钥的直接单向认证方法

（1）发送方知道接收方的公钥，才有可能实现机密性保护。例如下面的协议仅提供机密性：

A→B：$E_{PKB}[K_S] \| E_{KS}[M]$（$K_S$ 为 A 向 B 发送的一次通信密钥）。

（2）接收方知道发送方的公钥，才有可能认证性保护。例如下面的协议仅提供认证性：

A→B：$M \| E_{SKA}[H(M)]$。

这时，为了使 B 确信 A 的公钥的真实性，A 还要向 B 发送的公钥证书：

A→B：$M \| E_{SKA}[H(M)] \| E_{SKAS}[T \| ID_A \| PK_A]$（$SK_{AS}$ 为认证服务器的公钥，$E_{SKAS}[T \| ID_A \| PK_A]$是 AS 给 A 签署的公钥证书）。

（3）发送方和接收方互相知道对方的公钥，即可提供机密性又可提供认证性，例如：

A→B：$E_{PKB}[M \| E_{SKA}[H(M)]]$

这时，为了使 B 确信 A 的公钥的真实性，A 还要向 B 发送的公钥证书：

A→B：$E_{PKB}[M \| E_{SKA}[H(M)]] \| E_{SKAS}[T_S \| ID_A \| PK_A]$。

2. 借助 KDC 的身份认证

1）*基本方法*

KDC 是进行加密通信双方共同信任的第三方。它可以为通信双方分配不同的加密密钥；当两个实体方要进行加密通信时，首先要向 KDC 提出通信申请； KDC 验证了双方对真实性后，就会为该次通话生成一个工作密钥——该次通话密钥，并用它所保存的通信双方的密钥加密后分别发送给各方，由他们用这个工作密钥进行加密会话。这样，每个用户只需要保存 KDC 为自己分配的一个用于解密工作密钥的密钥，无须保存太多的其他密钥，从而避免了用户之间进行密钥交换所固有的安全漏洞，并可以生成一次通话用一个工作密钥，提高了安全性能。但是其通信量较大，并且需要 KDC 具有较好的鉴别性能。

下面是一个通过 KDC 进行身份验证的基本过程。

① A→KDC：$ID_A \| ID_B$。

② KDC→A：$E_{SKAU}[ID_B \| PK_B]$（SK_{AU}是 KDC 的私钥）。

③ A→B：$E_{PKB}[N_A \| ID_A]$（N_A是 A 选择的一次性随机数）。

④ B→KDC：$ID_B \| ID_A \| E_{PKAU}[N_A]$（$PK_{AU}$是 KDC 的公钥）。

⑤ KDC→B：$E_{SKAU}[ID_A \| PK_A] \| E_{PKB}[E_{SKAU}[N_A \| K_S \| ID_B]]$（$K_S$是 KDC 为 A、B 分配的一次性会话密钥）。

⑥ B→A：$E_{PKA}[E_{SKAU}[N_A \| K_S \| ID_B] \| N_B]$。

⑦ A→B：$E_{KS}[N_B]$。

这个协议中使用了一次性随机数，所以不再要求各方时钟的同步。但是，这个协议不能抵御攻击者对 A 的假冒。请读者设法为此改进这个协议。

2）相互认证协议 Needham-Schroeder

借助 KDC 进行单密钥分配，通常采用如下 5 步过程。

① A→KDC：$ID_A \| ID_B \| N_A$（A 请求与 B 加密通信）。

② KDC→A：$E_{KA}[K_s \| ID_B \| N_A \| E_{KB}[K_s \| ID_A]]$（A 获得了 K_s）。

③ A→B：$E_{KB}[K_s \| ID_A]$（B 安全地获得了 K_s）。

④ B→A：$E_{Ks}[N_B]$（B 知道 A 已掌握 K_s，用加密 N_2 向 A 示意自己也获得了 K_s）。

⑤ A→B：$E_{Ks}[f(N_B)]$。

这个协议被称为 Needham-Schroeder 协议。在这个协议中，前 3 步是 KDC 分发密钥，第④⑤两步是一个握手过程，即 B 认证 A 的过程：当在第⑤步中 B 能正确收到自己在第④步发出的 N_B 时，就可以证明 A 是当前的通话对象，因为自己在第③步获得的 K_s 是“新鲜”的，而非攻击者截获的前一次执行通话是用过的 K_s 的重放。但是，若攻击者已经获得旧会话密钥 K_s，并冒充 A 向 B 重放第③步的消息，就可以欺骗 B 使用旧 K_s 会话，接着截获第④步 B 的询问，再冒充 A 对 B 应答。这样就能冒充 A 向 B 发送假消息，使抗抵赖保护失效。

改进的办法是在②、③中加上一个时间戳，即

② KDC→A：$E_{KA}[K_s \| ID_B \| \boldsymbol{T} \| E_{KS}[K_s \| ID_A \| \boldsymbol{T}]]$

③ A→B：$E_{KB}[K_s \| ID_A \| \boldsymbol{T}]$

这样，A 和 B 都可以利用当前时间对 T 进行检查，以确定 K_S 是否陈旧。但是，使用这个协议的前提是 A 和 B 的时钟完全同步。若由于系统故障或存在计时误差，就会被攻击者利用时间差进行重放攻击。

重放攻击（replay attacks）又称重播攻击、回放攻击或新鲜性攻击（freshness attacks），是指攻击者发送一个目的主机已接收过的包，用欺骗手法破坏认证的正确性。

克服这一缺陷的方法，是将 Needham-Schroeder 协议进一步改进为：

① A→B：$ID_A \| N_A$

② B→KDC：$ID_B \| N_B \| E_{KB}[ID_A \| N_A \| T_B]$

③ KDC→A：$E_{KA}[ID_B \| N_A \| K_s \| ID_A \| T_B] \| E_{KB}[ID_A \| K_s \| T_B] \| N_B$

④ A→B：$E_{KB}[ID_A \| K_s \| T_B] \| E_{KS}[N_B]$

这个协议的执行过程如图 7.6 所示。

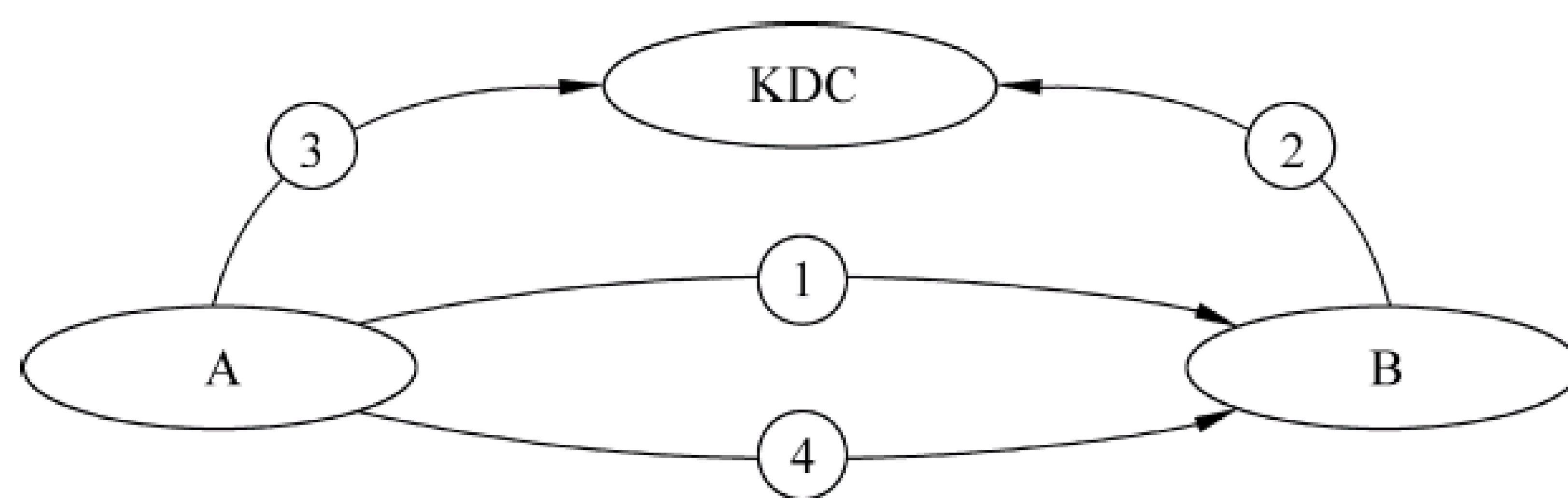


图 7.6　进一步改进的 Needham-Schroeder 协议

分析这个进一步改进的 Needham-Schroeder 协议，可以看出：

- 在第①步中，A 将 ID_A 和 N_A 以明文传送给 B；在第②步中，B 用自己和 KDC 共享的主密钥对 ID_A 和 N_A 加密传送给 KDC；在第③步中，KDC 对从 B 传来的信息解密，再用 KDC 与 A 共享的主密钥，将 K_s 和 N_A 一同加密传回 A。A 验证了 N_A 就可以知道，B 已经收到了 A 在第①步中发送的消息，同时也确信 K_s 是新鲜的。
- 在第②步中，B 将 ID_B 和 N_B 以明文传送给 KDC，经第③步由 KDC 将 N_B 传送给 A，再由 A 用 K_s 加密 N_B 将传回 B。同 N_A 的作用一样，N_B 用来保证 B 收到的 K_s 是新鲜的。
- 在第②步中，B 发出的 T_B 是 B 建议的证书截止时间，它是 B 根据自己的时钟确定的，不要求各方之间同步。
- $E_{KB}[ID_A \| N_A \| T_B]$经 KDC 传送给 A，由 A 留作以后认证的证据，并可以在有效时间范围内，不借助认证服务器（KDC）而是通过以下几步实现双方的新认证：

① A→B：$E_{KB}[ID_A \| K_s \| T_B], N_A'$

② B→A：N_B'，$E_{KS}[N_A']$

③ A→B：$E_{KS}[N_B']$

这里，B 通过 T_B 检验证据是否过时，而新产生的随机数 N_A'和 N_B'可以用来保证没有重放攻击。

3）单向认证协议

基于单向保密通信的特点，在 Needham-Schroeder 协议中去掉第④步和第⑤步，就成为能满足单向通信两个基本要求的单向认证协议：

① A→KDC：$ID_A \| ID_B \| N_A$

② KDC→A：$E_{KA}[K_s \| ID_B \| N_A \| E_{KB}[K_s \| ID_A]]$

③ A→B：$E_{KB}[K_s \| ID_A] \| E_{Ks}[M]$

这个协议提供了对于发送方 A 的认证，保证只有 B 才能阅读报文。但是，它不能防止重放攻击。为此，可以使用时间戳。不过由于电子邮件处理的延迟性，时间戳的作用有限。

7.3.4　基于数字证书的身份认证

1. 数字证书的特点

数字证书，也称数字身份证、数字 ID，其实就是一个特殊的计算机文件，这个计算机文件由权威机构——认证中心（Certificate Authority，CA）制作，用于向网上用户提供一组数字信息，包含用户身份信息、用户公开密钥、签名算法标识、证书有效期、证书序列号、颁证单位、扩展项等。数字证书有以下特点：

（1）它包含了身份信息，因此可以用于证明用户身份；

（2）它包含了非对称密钥，不但可用于数据加密，还可用于数据签名，保证通信过程的安全和不可抵赖；

（3）由于是权威机构颁布的，因此具有很高的公信度。

有了数字证书之后，在网上通信的双方进行联系的第一步便是利用预装在浏览器中的安全认证软件和认证中心的公钥对通信对象的数字证书进行验证；验证无误后，才可使用认证中心传递的加密公钥进行加密通信。

2. 基于数字证书的 USB Key

基于数字证书的智能卡，是用智能卡作为数字证书的存储介质，可以保证数字证书不被复制，并可以实现数字证书的所有功能。中国农业银行的 U 盾（见图 7.7）实际上是一种基于数字证书的 USB Key。它不仅可以履行数字证书的功能，进行双因子认证，还可以自动生成一个随机布局的软键盘，供用户输入自己的 PIN，从多个角度保障客户账户安全。



图 7.7　中国农业银行的 U 盾

3. 数字证书分类

常见的数字证书有以下几种：

（1）Web 服务器证书——用于在 Web 服务器与用户浏览器之间建立安全连接通道。

（2）服务器身份证书——提供服务器身份信息、公钥和 CA 签名，用于确保与其他服务器或用户通信的安全。

（3）计算机证书——提供计算机的身份信息，确保与其他计算机通信的安全性。

（4）个人证书——提供证书持有人的个人身份信息、公钥和 CA 签名，用于在网络中标识个人身份。浏览器证书也是一种个人证书。

（5）安全电子邮件证书——提供证书持有者的电子邮件地址、公钥和 CA 签名，用于电子邮件的安全传递和认证。

（6）企业证书——提供企业的身份信息、公钥和 CA 签名，用于在网络中标识证书持有者的身份。

（7）代码签名证书——附加在软件代码中，用于证实软件真实性，保护软件代码完整性的数字证书。

4. 认证中心

认证中心是可以信赖的第三方机构，它具有如下一些功能：

（1）颁发证书，如密钥对的生成，私钥的保护等，并保证证书持有者应有不同的密钥对。

（2）管理证书，记录所有颁发过的证书，以及所有被吊销的证书。

（3）用户管理，对于每一个新提交的申请，都要和列表中现存的标识名相比照，如出

现重复，就予以拒绝。

（4）吊销证书，在证书有效期内使其无效，并发表 CRL。

（5）验证申请者身份，对每一个申请者进行必要的身份认证。

（6）保护证书服务器，证书服务器必须是安全的，CA 应采取相应措施保证其安全性。例如，加强对系统管理员的管理、防火墙保护等。

（7）保护 CA 私钥和用户私钥，CA 签发证书所用的私钥要受到严格的保护，不能被毁坏，也不能非法使用。同时，要根据用户密钥对的产生方式，CA 在某些情况下有保护用户私钥的责任。

（8）审计与日志检查，为了安全起见，CA 对一些重要的操作应记入系统日志。在 CA 发生事故后，要根据系统日志做善后追踪处理——审计。CA 管理员要定期检查日志文件，尽早发现可能的隐患。

7.4 安 全 协 议

对于计算机网络来说，安全协议是保障信息安全的通信协议。计算机网络的安全协议都是基于密码技术的，其前提是：协议的参与者可能是可以信任者，也可能是攻击者或完全不信任者。

按照功能，安全协议一般可以分为如下 3 类。

（1）密钥交换协议：完成会话密钥建立。

（2）认证协议：包括身份认证、消息认证、数据源认证、数据目的认证等，可以防止假冒、篡改、否认等攻击。

（3）不可否认协议。

安全协议可以在网络的各层设计和实施。本节将介绍几种典型的安全协议。

7.4.1 SSH

1. SSH 概述

传统的网络服务程序，如 FTP、POP 和 Telnet 在传输机制和实现原理上没有考虑安全机制，它们在网络上用明文传送数据、用户账号和用户口令，别有用心的人通过窃听等网络攻击手段非常容易地就可以截获这些数据、用户账号和用户口令。而且，这些网络服务程序只有简单的安全验证，很容易受到“中间人”（man-in-the-middle）攻击——别有用心者在用户和目的服务器中间，首先冒充目的服务器接收用户传送给服务器的数据，然后再冒充传送数据的用户把数据传给真正的服务器，并往往会在数据上做些手脚。

SSH（Secure SHell）可以把所有传输的数据进行加密，不仅使“中间人”攻击无法实现，也能够防止 DNS 欺骗和 IP 欺骗。此外，使用 SSH 传输的数据是经过压缩的，因而可以加快传输的速度。

SSH 有很多功能，它既可以代替 Telnet，又可以为 FTP、POP、甚至为 PPP 提供一个安全的通道。

2．SSH 的应用

SSH 提供了很强的验证（authentication）机制与非常安全的通信环境，它最常见的应用就是用来取代传统的 Telnet、FTP 等网络应用程序。

SSH 可以通过“端口转发”在本地主机和远程服务器之间设置“加密通道”，并且这些“加密通道”可以与常见的 POP 应用程序、X 应用程序、Linuxconf 应用程序相结合，提供安全保障。

7.4.2　安全套接层协议

安全套接层协议（Security Socket Layer，SSL）是网景（Netscape）公司提出的构建在 TCP 之上、应用层之下、基于 Web 应用的安全协议，它的功能包括服务器认证、客户认证（可选）、SSL 链路上的数据完整性和 SSL 链路上的数据保密性。

1．SSL 体系结构

如图 7.8 所示，SSL 体系由两层组成。



图 7.8　SSL 体系结构

1）握手层（管理层）

握手层用于密钥的协商和管理，由握手协议、密钥更改协议和报警协议组成。

- SSL 握手协议（Handshake Protocol）：准许服务器端与客户端在开始传输数据前，可以通过特定的加密算法相互鉴别。
- SSL 更改密码说明协议（Change Cipher Spec）：保证可扩展性。
- SSL 警告协议（Alert Protocol）：产生必要的警告信息。

2）记录层

运行 SSL 记录协议（Record Protocol），为高层应用协议提供各种安全服务，对上层数据进行加密、产生 MAC 等并进行封装。

2．SSL 的工作过程

（1）安全协商：互相交换 SSL 版本号和所支持的加密算法等信息。

（2）彼此认证。

① 服务器将自己由 CA 颁发的私钥所加密的证书发给浏览器。服务器也可以向浏览器发出证书请求，对浏览器进行认证。

② 浏览器检查服务器的证书（是否由自己列表中的某个 CA 颁发）：不合法，则终止连接；合法，则生成会话密钥。

③ 如果服务器有证书请求，浏览器也要发送自己的证书。

（3）生成会话密钥。

① 浏览器用 CA 的公钥对服务器的证书解密，获得服务器的公钥。

② 浏览器生成一个随机会话密钥，用服务器的公钥加密后，发送给服务器。

（4）启动会话密钥。

① 浏览器向服务器发送消息：告诉服务器以后自己发送的信息将用协商好的会话密钥加密。

② 浏览器再向服务器发送一个加密消息：告诉服务器会话协商过程完成。

③ 服务器向浏览器发送消息：告诉浏览器以后自己发送的信息将用协商好的会话密钥加密。

④ 服务器再向浏览器发送一个加密消息：告诉浏览器会话协商过程完成。

（5）SSL 会话正式开始：双方用协商好的会话密钥加密发送的消息。

对于电子商务应用来说，使用 SSL 可保证信息的真实性、完整性和保密性。但由于 SSL 不对应用层的消息进行数字签名，因此不能提供交易的不可否认性，这是 SSL 在电子商务中使用的最大不足。有鉴于此，网景公司在从 Communicator 4.04 版开始的所有浏览器中引入了一种被称作“表单签名（Form Signing）”的功能，在电子商务中，可利用这一功能来对包含购买者的订购信息和付款指令的表单进行数字签名，从而保证交易信息的不可否认性。

7.4.3　IPSec 与虚拟专用网

IPSec（IP Security）是在网络层提供的安全服务协议，是一套协议包，它把多种安全技术集合到一起，可以防止 IP 地址欺骗，防止任何形式的 IP 数据包篡改和重放，并为 IP 数据包提供机密性和其他安全服务。

IPSec 的一个基本应用是建立 VPN（Virtual Private Network，虚拟专用网）。VPN 是指将物理上分布在不同地点的专用网络，通过不可信任的公共网络构造成逻辑上的虚拟子网，进行安全的通信。这里公共网络主要指 Internet。如图 7.9 所示为 VPN 的示意图。

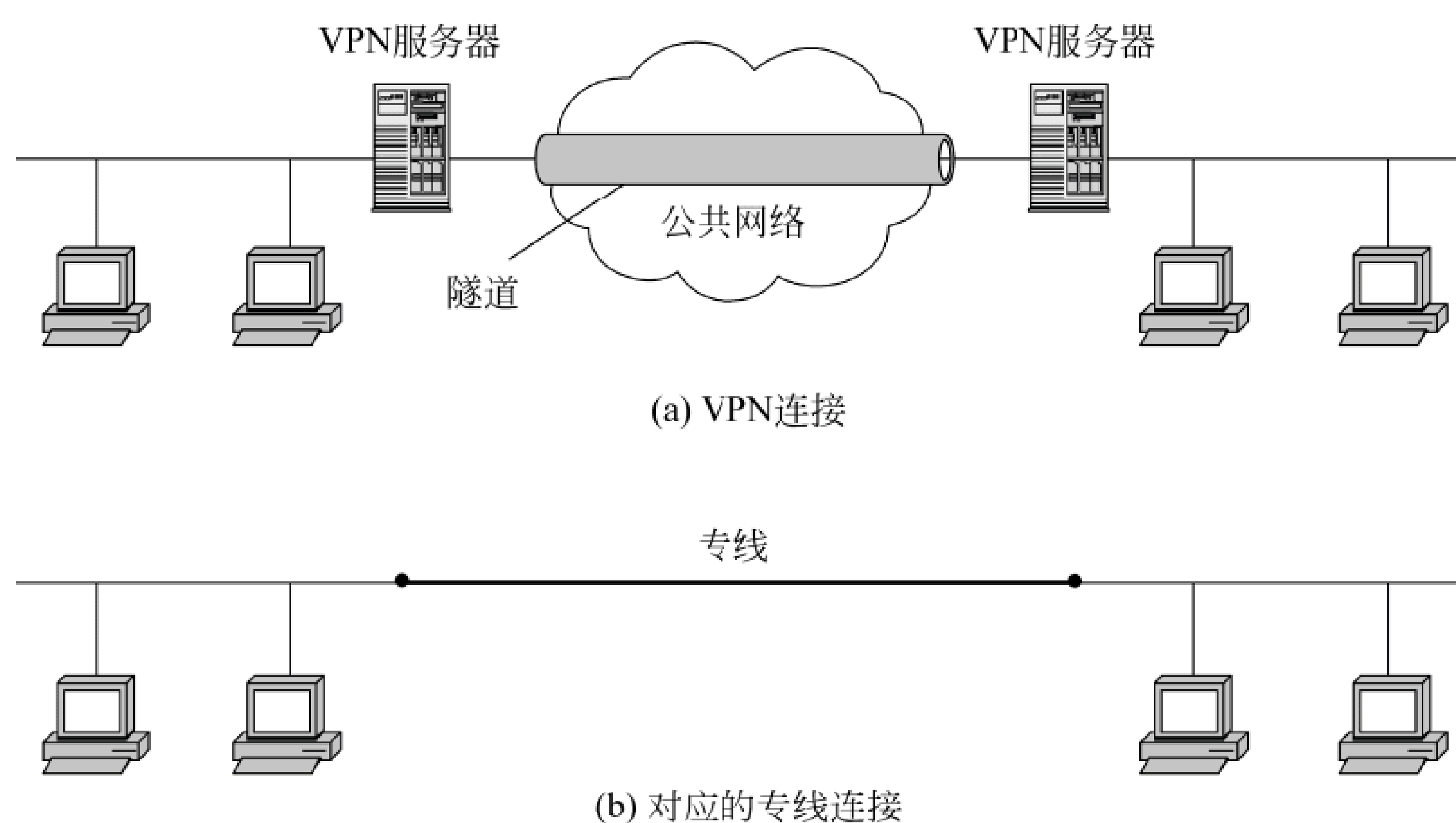


图 7.9　VPN 的作用

VPN 技术采用了加密、认证、存取控制、数据完整性等措施，相当于在各 VPN 设备间形成一些跨越 Internet 的虚拟通道——“隧道”，使得敏感信息只有预定的接收者才能读懂，实现信息的安全传输，使信息不被泄露、篡改和复制。

7.5　网络隔离技术

7.5.1　数据包过滤

1. 数据包过滤基本准则

最早的包过滤是在路由器上进行的。通过对路由表的配置，来决定数据包是否符合过滤规则。数据包的过滤规则由一些规则逻辑描述：一条过滤规则规定了允许数据包流进或流出内部网络的一个条件。在制定了数据包过滤规则后，对于每一个数据包，路由器会从第一条规则开始逐条进行检查，最后决定该数据包是否符合过滤逻辑。

数据包规则的应用有两种策略：

（1）默认接受——一切未被禁止的，就是允许的。即除明确指定禁止的数据包外，其他都是允许通过的。这也称为“黑名单”策略。

（2）默认拒绝——一切未被允许的，就是禁止的。即除明确指定通过的数据包外，其他都是被禁止的。这也称为“白名单”策略。

从安全的角度，默认拒绝应该更可靠。

此外，包过滤还有禁入和禁出的区别。前者不允许指定的数据包由外部网络流入内部网络，后者不允许指定的数据包由内部网络流入外部网络。

2. 地址过滤策略

按照地址进行过滤是最简单的过滤方式，它的过滤规则只对数据包的源地址、目标地址和地址偏移量进行判断，这在路由器上是非常容易配置的。对于信誉不好或内容不宜并且地址确定的主机，用这种策略通过简单配置，就可以将其拒之门外。

例 7.1　某公司有一B类网(123.45)。该网的子网(123.45.6.0/24)有一合作网络(135.79)。管理员希望：

（1）禁止一切来自 Internet 的对公司内网的访问；

（2）允许来自合作网络的所有子网（135.79.0.0/16）访问公司的子网（123.45.6.0/24）；

（3）禁止对合作网络的子网（135.79.99.0/24）的访问权（对全网开放的特定子网除外）。

由这些需求可以制定出如表 7.1 所示的包过滤规则。为简单起见，只考虑从合作网络流向公司的数据包，对称地处理逆向数据包只需互换规则行中源地址和目标地址即可。

表 7.1　某公司网络的包过滤规则

规　则	源　地　址	目　的　地　址	过滤操作
A	135.79.0.0/16	123.45.6.0/24	允许
B	135.79.99.0/24	123.45.0.0/16	拒绝
C	0.0.0.0/0	0.0.0.0/0	拒绝

表中规则 C 是默认规则。

表 7. 2 是使用一些样本数据包对如表 7.1 所示的过滤规则的测试结果。

表 7.2　使用样本数据包测试结果

数据包	源地址	目的地址	目标行为操作	ABC 行为操作	BAC 行为操作
1	135.79.99.1	123.45.1.1	拒绝	拒绝(B)	拒绝(B)
2	135.79.99.1	123.45.6.1	允许	允许(A)	拒绝(B)
3	135.79.1.1	123.45.6.1	允许	允许(A)	允许(A)
4	135.79.1.1	123.45.1.1	拒绝	拒绝(C)	拒绝(C)

由表 7.2 可见，按 ABC 的规则顺序，能够得到想要的操作结果；而按 BAC 的规则顺序则得不到预期的操作结果，原本允许的数据包 2 被拒绝了。

仔细分析可以发现，表 7.1 中用来禁止合作网的特定子网的访问规则 B 是不必要的。它正是在 BAC 规则集中造成数据包 2 被拒绝的原因。如果删除规则 B，可得到如表 7.3 所示的行为操作。

表 7.3　删除规则 B 后的行为操作

数据包	源地址	目的地址	目标行为操作	AC 行为操作
1	135.79.99.1	123.45.1.1	拒绝	拒绝(C)
2	135.79.99.1	123.45.6.1	允许	允许(A)
3	135.79.1.1	123.45.6.1	允许	允许(A)
4	135.79.1.1	123.45.1.1	拒绝	拒绝(C)

这才是想要的结果。由此得出两点结论：

- 正确地制定过滤规则是困难的；
- 过滤规则的重新排序使得正确地指定规则变得越发困难。

3. 数据包的服务过滤

按服务进行过滤，就是根据 TCP/UDP 的端口号制定过滤策略。但是，由于源端口是可以伪装的，所以基于源端口的过滤是有风险的。同时还需要确认内部服务确实是在相应的端口上。下面进行一些分析。

例 7.2　表 7.4 与表 7.5 就是否考虑数据包的源端口进行对照。表 7.4 由于未考虑到数据包的源端口，出现了两端所有端口号大于 1024 的端口上的非预期的作用。而表 7.5 考虑到数据包的源端口，所有规则限定在 25 号端口上，故不可能出现两端端口号均在 1024 以上的端口上连接的交互。

表 7.4　未考虑源端口时的包过滤规则

规则	方向	类型	源地址	目的地址	目的端口	行为操作
A	入	TCP	外	内	25	允许
B	出	TCP	内	外	>=1024	允许
C	出	TCP	内	外	25	允许
D	入	TCP	外	内	>=1024	允许
E	出/入	任何	任何	任何	任何	禁止

表 7.5　考虑了源端口时的包过滤规则

规则	方向	类型	源地址	目的地址	源端口	目的端口	行为操作
A	入	TCP	外	内	>=1024	25	允许
B	出	TCP	内	外	25	>=1024	允许
C	出	TCP	内	外	>=1024	25	允许
D	入	TCP	外	内	25	>=1024	允许
E	出/入	任何	任何	任何	任何	任何	禁止

4. 数据包的内容过滤策略

内容安全是包过滤技术中正在兴起的一个重要的分支，也是目前最活跃的安全领域。它是基于内容安全的一项技术。

内容安全措施因内容性质而异，主要分为如下 3 种情况。

1）违禁内容的传播及其策略

违禁内容是指内容本身要表达的意思违反了某种规则或安全策略，尤其是政策法规允许的范畴。例如，散布关于瘟疫、地震、恐怖袭击等谣言，制造或传播淫秽色情等内容，都是违法的。违禁内容的危害是对思想造成破坏。在很多情况下，违禁内容的表达方式和格式并没有什么特殊之处，因此无法从表达方式或格式方面加以禁止。常用的策略有两个方面。一是对违禁内容进行内容过滤，如基于关键词的内容过滤，基于语义的内容过滤。前者在技术上很成熟，准确度很高，漏报率低，但误报率高。二是对违禁内容的来源进行访问控制，这种方式对已经知道恶意传播的对象非常有效。到目前为止，在必须执行违禁内容控制的情况下，多采用人工和技术相结合的策略。

2）基于内容的破坏及其策略

内容破坏的典型是带有病毒的文件，是被篡改了的正常文件上带有病毒特征代码。这些代码在被执行的时候，具有有害的特性。防病毒是目前采用最多的防止基于内容破坏的解决方案。通过查找内容中的恶意病毒代码来消除基于内容的破坏。防病毒软件同样存在漏报和误报的问题。最关键的问题是，每次总是病毒爆发在前，才能取得病毒特征代码，然后才能防止该病毒。预防已知病毒的实现较为成功，但预防未知病毒的能力较弱。为了弥补防病毒软件这方面的不足，出现了很多的相关技术，如专家会诊、引发病毒隔离区等，来补充和弥补防病毒软件的不足。

3）基于内容的攻击及其策略

基于内容的攻击已经超过违禁内容传播和病毒，成为目前最热门的威胁之一。目前存在的十大漏洞和风险包括参数无效、访问控制失效、账户和会话管理失效、跨站点脚本、缓冲溢出、恶意命令、错误处理问题、不安全加密、远程管理缺陷、配置错误。目前已经出现一类新的产品称为应用安全代理来解决基于内容攻击的问题。

与传统的过滤方法相比，基于内容的过滤技术需要耗费更多的计算资源。如何突破内容过滤的性能瓶颈，已经成为用户和厂商普遍关心的问题。

7.5.2　网络地址转换

网络地址转换（Network Address Translation，NAT）就是使用两套 IP 地址——内部 IP 地址（也称私有 IP 地址）和外部 IP 地址（也称公共 IP 地址）。当受保护的内部网连接到 Internet 并且有用户要访问 Internet 时，它首先使用自己网络的内部 IP 地址，到了 NAT 后，NAT 就会从公共 IP 地址集中选一个未分配的地址分配给该用户，该用户即可使用这个合法的 IP 地址进行通信。同时，对于内部的某些服务器，如 Web 服务器，网络地址转换器允许为其分配一个固定的合法地址。外部网络的用户就可通过 NAT 来访问内部的服务器。这种技术既缓解了少量的 IP 地址和大量的主机之间的矛盾——被保护网络中的主机不必拥有固定的 IP 地址；又对外隐藏了内部主机的 IP 地址，提高了安全性。

NAT 的工作过程如图 7.10 所示。

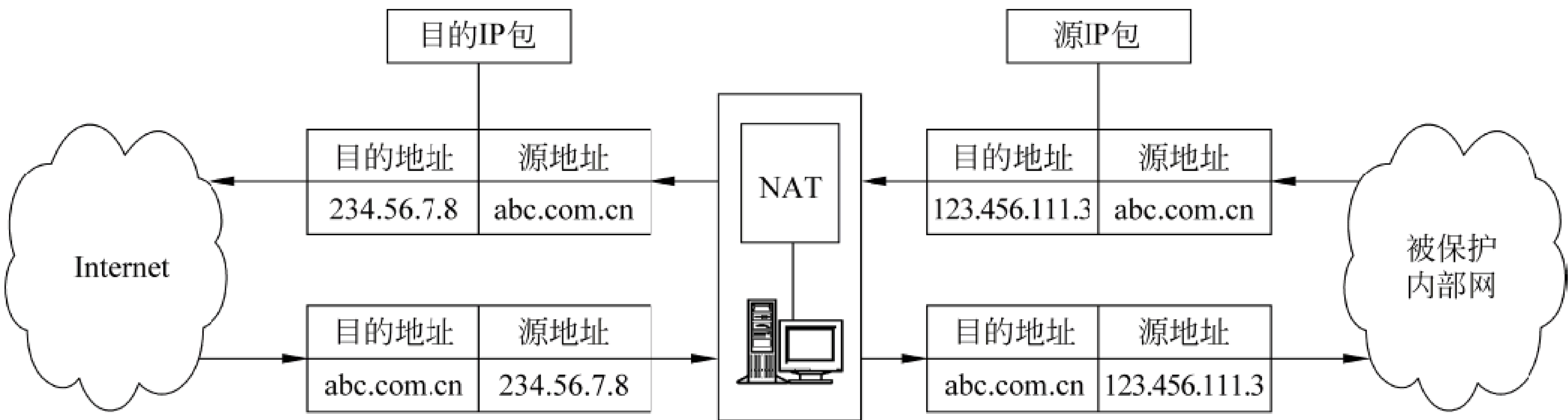


图 7.10　NAT 的工作过程

在内部网络通过安全网卡访问外部网络时，将产生一个映射记录。系统将外出的源地址和源端口映射为一个伪装的地址和端口，让这个伪装的地址和端口通过非安全网卡与外部网络连接，这样对外就隐藏了真实的内部网络地址。在外部网络通过非安全网卡访问内部网络时，它并不知道内部网络的连接情况，而只是通过一个开放的 IP 地址和端口来请求访问。NAT 据预先定义好的映射规则来判断这个访问是否安全：当符合规则时，防火墙认为访问是安全的，可以接受访问请求，也可以将连接请求映射到不同的内部计算机中；当不符合规则时，则认为该访问是不安全的，不能被接受，外部的连接请求即被屏蔽。网络地址转换的过程对于用户来说是透明的，不需要用户进行设置，用户只要进行常规操作即可。

7.5.3　代理技术

应用于网络安全的代理（Proxy）技术，来自代理服务器（Proxy Server）技术。代理服务器是用户计算机与 Internet 之间的中间代理机制，它采用客户机/服务器工作模式。代理服务器位于客户与 Internet 上的服务器之间。请求由客户端向服务器发起，但是这个请求要首先被送到代理服务器；代理服务器分析请求，确定其是合法的以后，首先查看自己的缓存中有无要请求的数据，有就直接传送给客户端，否则再以代理服务器作为客户端向远程的服务器发出请求；远程服务器的响应也要由代理服务器转交给客户端，同时代理服务器还将响应数据在自己的缓存中保留一份副本，以备客户端下次请求时使用。图 7.11 为代理服务的结构及其数据控制和传输过程示意图。

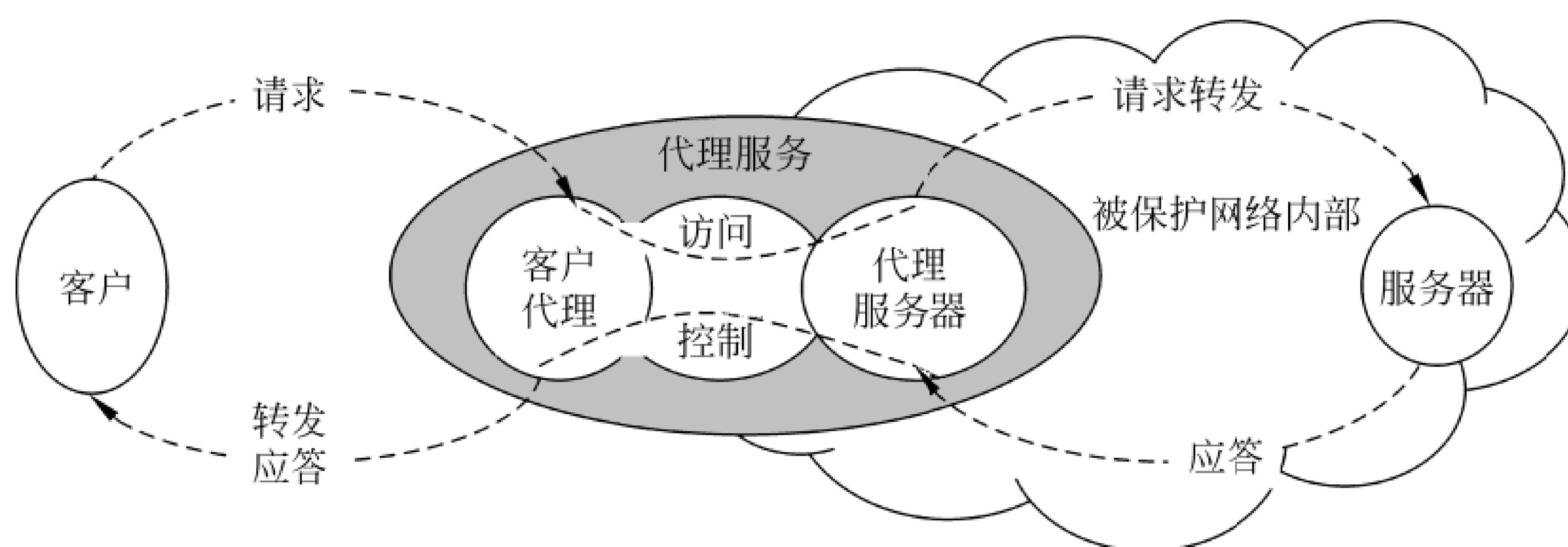


图 7.11　代理服务的结构及其数据控制和传输过程

应用于网络安全的代理技术，也是要建立一个数据包的中转机制，并在数据的中转过程中，加入一些安全机制。

代理技术可以在不同的网络层次上进行，分别称为应用级代理和电路级代理。它们的工作原理有所不同。

1. 应用级代理

1）应用级代理的基本原理

图 7.12 为其示意图。只有为特定的应用程序安装了代理程序代码，该服务是才会被支持，并建立相应的连接。显然，这种方式可以拒绝任何没有明确配置的连接，从而提供了额外的安全性和控制性。但是，应用级代理没有通用的安全机制和安全规则描述，它们通用性差，对不同的应用具有很强的针对性和专用性。

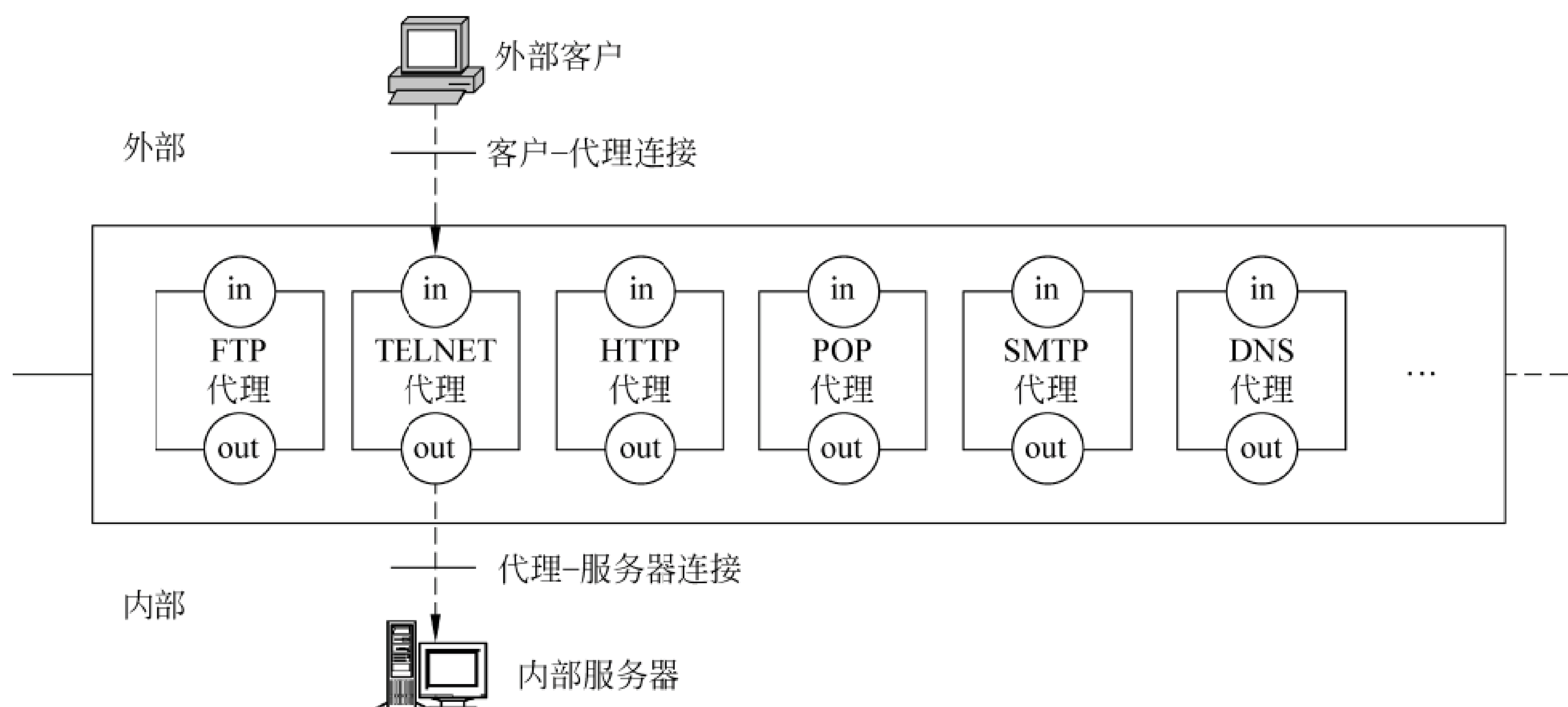


图 7.12　应用级代理工作原理

图 7.13 为应用级代理的基本工作过程。

2）应用级代理的功能

（1）阻断路由与 URL。代理服务是一种服务程序，它位于客户机与服务器之间，完全阻挡了二者间的数据交流。从客户机来看，代理服务器相当于一台真正的服务器；而从服务器来看，代理服务器又是一台真正的客户机。当客户机需要使用服务器上的数据时，首先将数据请求发给代理服务器，代理服务器再根据这一请求向服务器索取数据，然后再由代理服务器将数据传输给客户机。由于外部系统与内部服务器之间没有直接的数据通道，

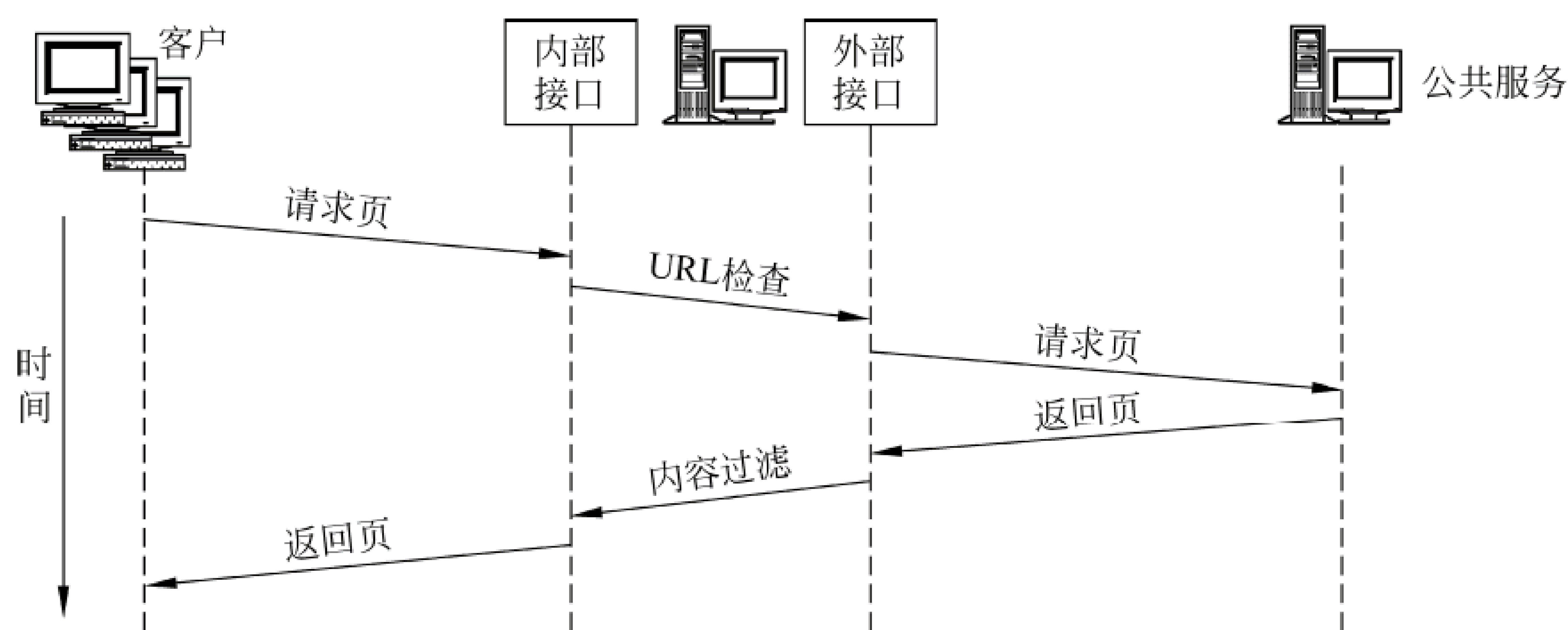


图 7.13　应用级代理的基本工作过程

外部的恶意侵害也就很难伤害到企业内部的网络系统。

代理是通过侦听网络内部客户的服务请求，然后把这些请求发向外部网络。在这一过程中，代理要重新产生服务级请求。例如，一个 Web 客户向外部发出一个请求时，这个请求会被代理服务器"拦截"，再由代理服务器向目标服务器发出一个请求。服务协议（如 HTTP）才可以通过代理服务器，而 TCP/IP 和其他低级协议不能通过，必须由代理服务器重新产生。因此外部主机与内部机器之间并不存在直接连接，从而可以防止传输层因源路由、分段和不同的服务拒绝造成的攻击，确保没有建立代理服务的协议不会被发送的外部网络。

（2）隐藏客户。应用级代理既可以隐藏内部 IP 地址，也可以给单个用户授权，即使攻击者盗用了一个合法的 IP 地址，也通不过严格的身份认证。因此应用级代理比数据包过滤具有更高的安全性。但是这种认证使得应用网关不透明，用户每次连接都要经过认证，这给用户带来了许多不便。这种代理技术需要为每个应用写专门的程序。

（3）安全监控。代理保证所有内容都经过单一的一个点，该点称为网络数据的一个检查点。在应用级代理提供授权检查及代理服务。大多数代理软件具有对过往的数据包进行分析监控、注册登记、过滤、记录和报告等功能。当外部某台主机试图访问受保护网络时，必须先在代理上经过身份认证。通过身份认证后，再运行一个专门为该网络设计的程序，把外部主机与内部主机连接起来。在这个过程中，可以对用户访问的主机、访问时间及访问的方式进行记录、监控。同样，受保护网络的内部用户访问外部网时也需先登录到代理上，通过验证后，才可访问。当发现被攻击迹象时会向网络管理员发出警报，并能保留攻击痕迹。代理服务器的缺点是必须针对客户机可能产生的所有应用类型逐一进行设置，大大增加了系统管理的复杂性。此外，假如由于黑客攻击等原因使代理不工作时，对应的服务请求也就被切断了。这也是单点访问的不足之处。

由于应用级代理像横在客户与服务器连通路径上的一个关口，所以也被称为应用级网关。也由于应用级代理像横在客户与服务器连通路径上的一堵墙，所以也被称为应用级防火墙。

2. 电路级代理

电路级代理也称电路级网关。在 OSI 模型中电路级网关工作在会话层，进行会话层的

过滤。在 TCP/IP 体系中，电路级网关依赖于 TCP 连接，如图 7.14 所示，它只用来在两个通信端点之间转接，对数据包进行转发，进行简单的字节复制式的数据包转接，而数据包处理要在应用层进行。

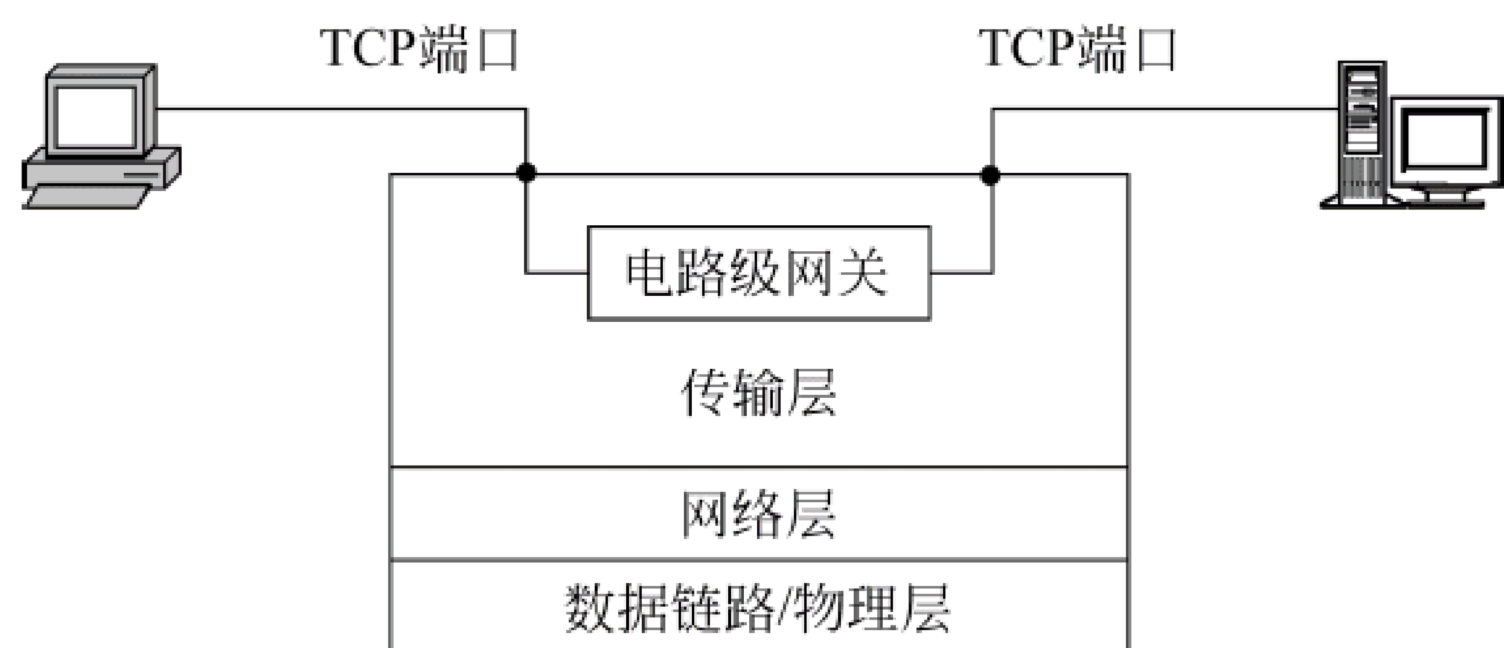


图 7.14　电路级网关工作原理

电路级网关对外像一个代理，对内又像一个过滤器。这种特点使它可以适用于多个协议，为各种不同的协议提供服务，但它不能解释应用协议。简单的电路级网关仅传输 TCP 的数据段，增强的电路级网关还具有认证作用。

7.5.4　网络防火墙

1. 防火墙及其基本功能

在建筑群中，防火墙（Fire Wall）用来防止火灾蔓延。在计算机网络中，防火墙是设置在可信任的内部网络和不可信任的外界之间的一道屏障，来保护计算机网络的资源和用户的声誉,使一个网络不受来自另一个网络的攻击。

在逻辑上，防火墙是一个分离器、一个限制器，也是一个分析器，它有效地监控了内部网和 Internet 之间的全部活动，保证了内部网络的安全。

在技术上，防火墙就是基于上述技术的网络安全“站”。它作为一个中心“遏制点”，可以将局域网的安全管理集中起来，屏蔽非法请求，防止跨权限访问并产生安全报警。具体地说，防火墙具有以下一些功能。

1）作为网络安全的屏障

防火墙由一系列的软件和硬件设备组合而成，它保护网络中有明确闭合边界的一个网块，所有进出该网块的信息，都必须经过防火墙，将发现的可疑访问拒之门外。当然，防火墙也可以防止未经允许的访问进入外部网络。因此，防火墙的屏障作用是双向的，即进行内外网络之间的逻辑隔离，包括地址数据包过滤、代理和地址转换。

2）防止攻击性故障蔓延和内部信息的泄露

防火墙也能够将隔开网络中一个网块（也称网段）与另一个网块隔开，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。此外，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些被透露的内部细节，如 Finger、DNS 等服务。

3）强化网络安全策略

防火墙能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上，形

成以防火墙为中心的安全方案。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如在网络访问时，一次一密口令系统和其他的身份认证系统完全可以不必分散在各个主机上，而集中于防火墙一身。

4）MAC 与 IP 地址的绑定

MAC 与 IP 地址绑定起来，主要用于防止受控（不可访问外网）的内部用户通过更换 IP 地址访问外网。这其实是一个可有可无的功能。不过因为它实现起来太简单了，在内部只需要两个命令就可以实现，所以绝大多数防火墙都提供了该功能。

5）对网络存取和访问进行监控审计

防火墙的审计和报警机制在防火墙体系中是很重要的，只有有了审计和报警，管理人员才可能知道网络是否受到了攻击。另外，防火墙的该功能也有很大的发展空间，如日志的过滤、抽取、简化等等。日志还可以进行统计、分析、（按照特征）存储（在数据库中），稍加扩展便又是一个网络分析与查询模块。如果所有的访问都经过防火墙，防火墙就能记录下这些访问并做出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。

6）流量控制（带宽管理）和统计分析、流量计费

流量控制可以分为基于 IP 地址的控制和基于用户的控制。基于 IP 地址的控制是对通过防火墙各个网络接口的流量进行控制，基于用户的控制是通过用户登录来控制每个用户的流量，从而防止某些应用或用户占用过多的资源，并且通过流量控制可以保证重要用户和重要接口的连接。流量统计是建立在流量控制基础之上的。一般防火墙通过对基于 IP、服务、时间、协议等内容进行统计，可以与管理界面实现挂接，实时或者以统计报表的形式输出结果。基于此，流量计费也是非常容易实现的。

7）远程管理

管理界面一般可完成对防火墙的配置、管理和监控。管理界面设计直接关系到防火墙的易用性和安全性。目前防火墙主要有两种远程管理界面：Web 界面和 GUI 界面。对于硬件防火墙，一般还有串口配置模块和/或控制台控制界面。

8）其他特殊功能

这些功能纯粹是为了迎合特殊客户的需要或者为赢得卖点而加上的。如限制同时上网人数，限制使用时间，限制特定使用者才能发送 E-mail，限制 FTP 只能下载文件不能上传文件，阻塞 Java、ActiveX 控件等。有些防火墙加入了查（清）毒功能。这些依需求不同而定。

2. 屏蔽路由器（Screening Router）和屏蔽主机（Screening Host）

防火墙最基本、也是最简单的技术是数据包过滤。过滤规则可以安装在路由器上，也可以安装在主机上。具有数据包过滤功能的路由器称为屏蔽路由器。具有数据包过滤功能的主机称为屏蔽主机。图 7.15 为包过滤防火墙的基本结构。

路由器是内部网络与 Internet 连接的必要设备，是一种“天然”的防火墙，它除具有路由功能之外，还可以安装分组/包过滤（数据包过滤或应用网关）软件，决定是否对到来的数据包要进行转发。这种防火墙实现方式相当简捷，效率较高，在应用环境比较简单的情

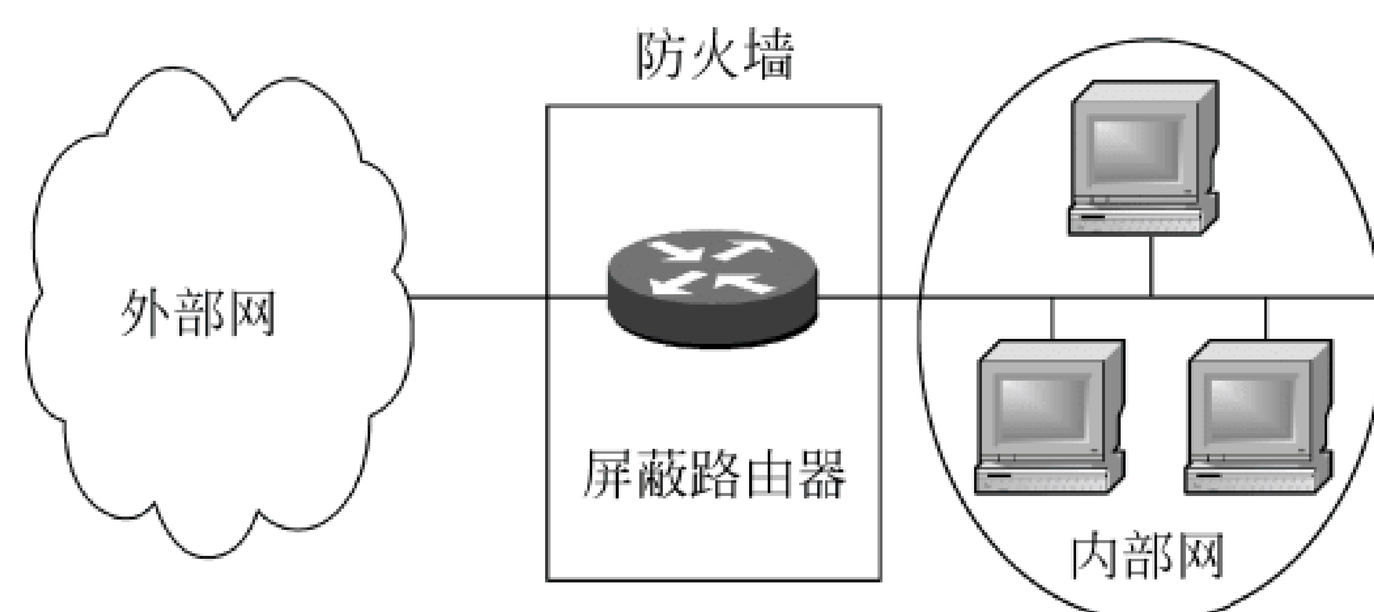


图 7.15　路由过滤式防火墙

况下，能够以较小的代价在一定程度上保证系统的安全。但由于过滤路由器是在网关之上的包过滤，因此它允许被保护网络的多台主机与 Internet 的多台主机直接通信。这样，其危险性便分布在被保护网络内的全部主机以及允许访问的各种服务器上，随着服务的增加，网络的危险性也增加。其次，也是特别重要的一点，是这种网络由于仅靠单一的部件来保护系统，一旦部件被攻破，就再也没有任何设防了，并且当防火墙被攻破时几乎可以不留下任何痕迹，甚至难以发现已发生的攻击。这时只能根据数据包的来源、目标和端口等网络信息进行判断，无法识别基于应用层的恶意侵入，如恶意的 Java 小程序以及电子邮件中附带的病毒。有经验的黑客也很容易伪造 IP 地址，骗过包过滤型防火墙，一旦突破防火墙，即可对主机上的软件和配置漏洞进行攻击。进一步说，由于数据包的源地址、目标地址以及 IP 的端口号都在数据包的头部，很有可能被窃听或假冒；并且数据包缺乏用户日志（log）和审计信息（audit），不具备登录和报告性能，不能进行审核管理，因而过滤规则的完整性难以验证，所以安全性较差。

3. 双宿主网关（Dual Homed Gateway）

如图 7.16 所示，双宿主主机是一台有两块 NIC 的计算机，每一块 NIC 各有一个 IP 地址。所以它可以采用 NAT 和代理两种安全机制。如果 Internet 上的一台计算机想与被保护网（Intranet）上的一个工作站通信，必须先行注册，与它能看到的 IP 地址联系；代理服务器软件通过另一块 NIC 启动到 Intranet 的连接。

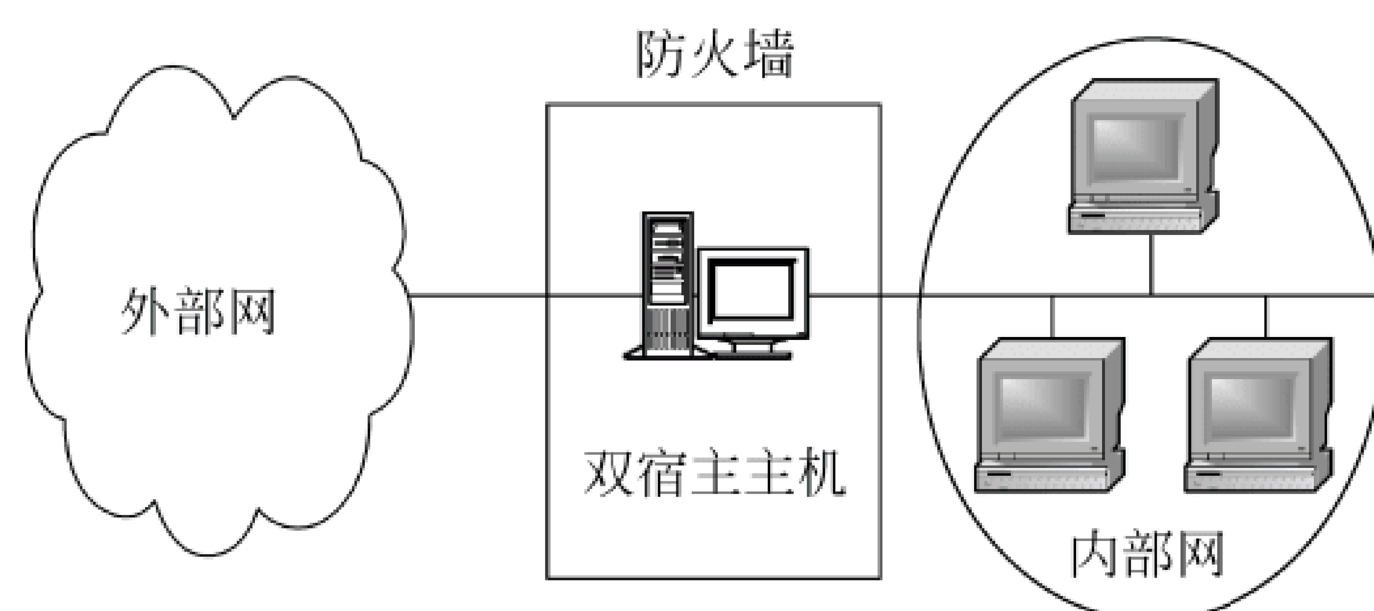


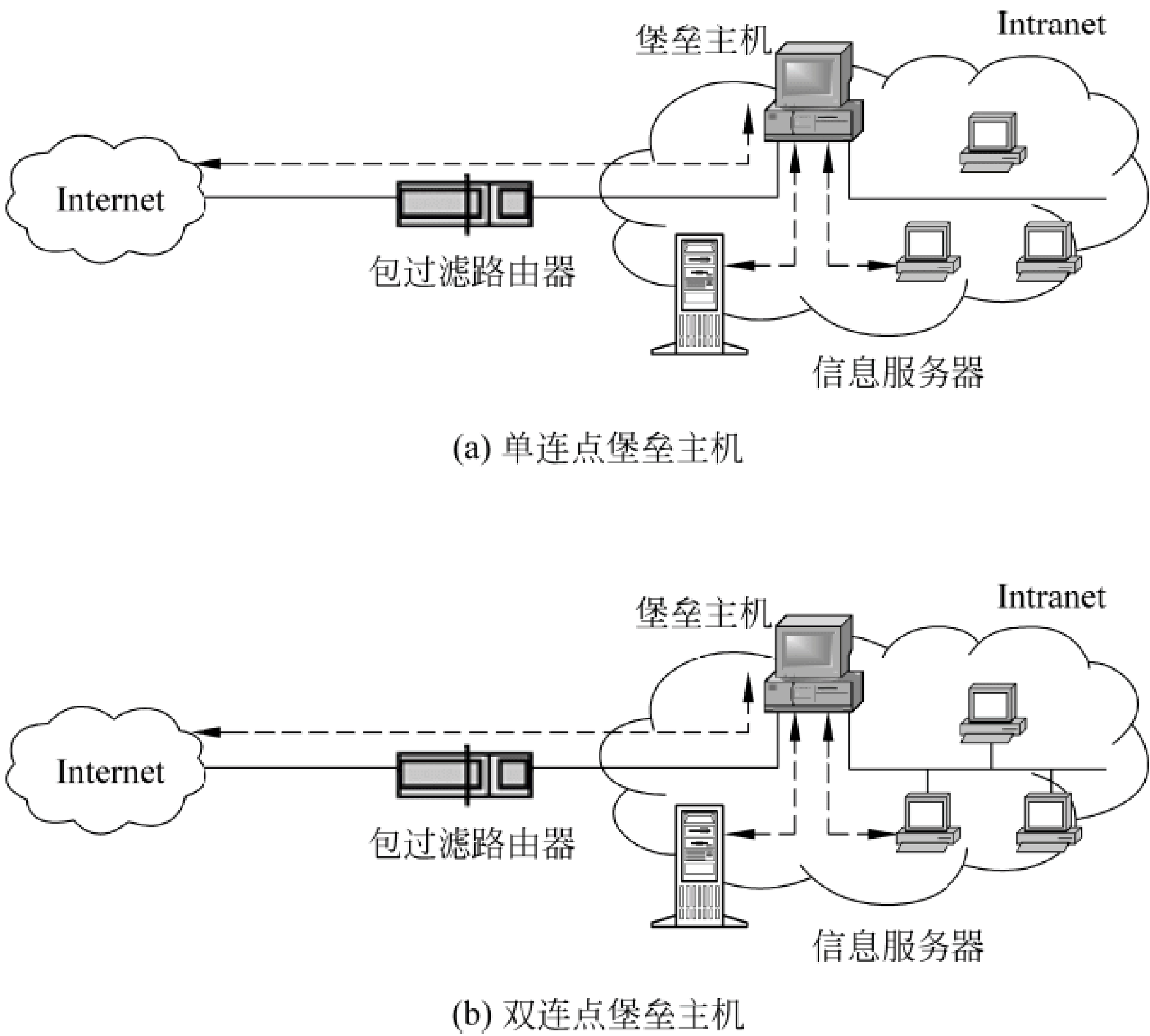
图 7.16　双宿主主机网关防火墙

双宿主网关使用代理服务器简化了用户的访问过程，它将被保护网络与外界完全隔离，域名系统的信息不会通过被保护系统传到外部，所以系统的名字和 IP 地址对 Internet 是隐蔽的，做到了对用户全透明。由于该防火墙仍是由单机组成，没有安全冗余机制，一旦该“单失效点”出问题，网络将无安全可言。

4. 堡垒主机（Bastion Host）

堡垒主机是专门暴露在外部网络上的一台计算机，是被保护的内部网络在外网上的代表并作为进入内部网的一个检查点。它具有双重保护作用：使用过滤规则的配置使得外部主机只能访问堡垒主机，发往内部网的其他业务流则全部被阻塞，不允许外部访问被保护网络的其他资源，有较高的安全可靠性；另一方面，机构的安全策略可以决定允许内部系统直接访问外部网，还是要求使用配置在堡垒主机上的代理服务。当配置路由器的过滤规则使其仅可接收来自堡垒主机的内部业务流时，内部用户就不得不使用代理服务。

壁垒主机可分为单连点和双连点两种，如图 7.17 所示。可以看出，双连点堡垒主机过滤式防火墙比单连点堡垒主机过滤式防火墙有更高的安全等级。由于堡垒主机具有两个网络接口，除了外部用户可以直接访问信息服务器外，外部用户发往内部网络的业务流和内部系统对外部网络的访问都不得不经过堡垒主机，以提高附加的安全性。



(a) 单连点堡垒主机

(b) 双连点堡垒主机

图 7.17　堡垒主机过滤式防火墙的两种结构

在这种系统中，由于堡垒主机成为外部网络访问内部网络的唯一入口，所以对内部网络的可能安全威胁都集中到了堡垒主机上。因而对堡垒主机的保护强度，关系到整个内部网的安全。

5. 屏蔽子网（Screened Subnet）防火墙

在被保护网络和 Internet 之间设置一个独立的子网作为防火墙，就是子网过滤防火墙。具体的配置方法是在过滤主机的配置上再加上一个路由器，形成具有外部路由过滤器、内部路由过滤器、应用网关三道防线的过滤子网，如图 7.18 所示。

在子网过滤防火墙中，外部过滤路由器用于防范通常的外部攻击（如源地址欺骗和源路由攻击），并管理外部网到过滤子网的访问。外部系统只能访问到堡垒主机，通过堡垒主机向内部网传送数据包。内部过滤路由器管理过滤子网与内部网络之间的访问，内部系统

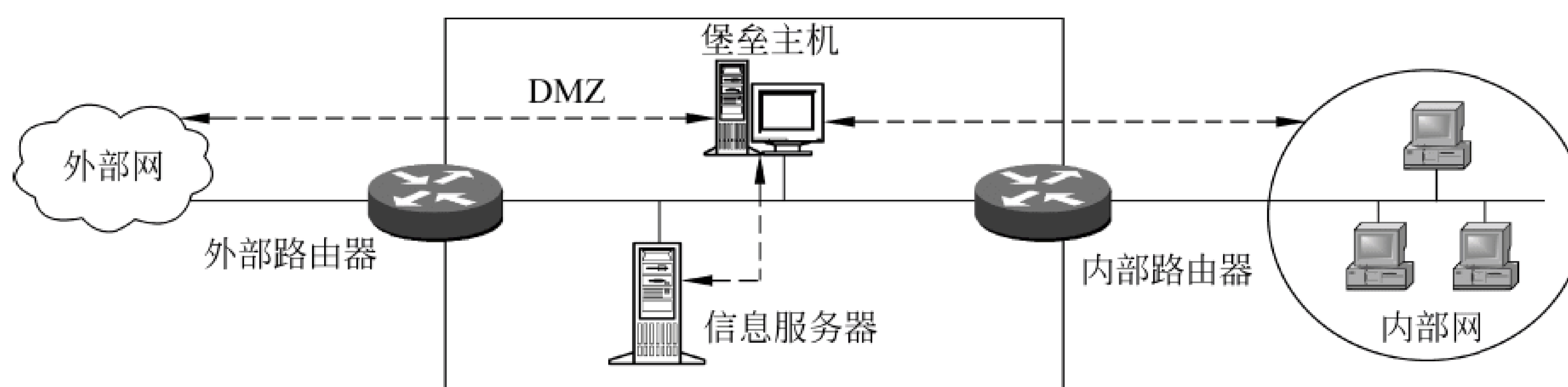


图 7.18　子网过滤防火墙配置

只能访问到堡垒主机，通过堡垒主机向外部网发送数据包。简单地说，任何跨越子网的直接访问都是被严格禁止的。从而在两个路由器之间定义了一个“非军事区”（Demilitarized Zone，DMZ）。这种配置的防火墙具有最高的安全性，但是它要求的设备和软件模块较多，价格较贵且相当复杂。

7.5.5　网络的物理隔离

20 世纪末，“政府上网”热潮把我国的信息化带进了一个新的高度。政府上网不仅表明 Internet 已经进入了一个非常重要的领域，而且为信息系统安全技术提出了新的课题。政府中有许多敏感的数据以及大量机密数据，也有最为国民关心的信息。目前虽然开发了各种防火墙、病毒防治系统以及入侵检测、安全预警、漏洞扫描等安全技术，但却并没有完全阻止入侵，内部网络被攻破的事件屡有发生，据统计有近半数的防火墙被攻破过。为此，国家保密局 2000 年 1 月 1 日起实施的《计算机信息系统国际联网保密管理规定》第二章第六条要求：“涉及国家机密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行物理隔离。”

基于这一规定，现在的电子政务网形成了如图 7.19 所示的三级网络结构：内网、外网和公网。其安全要求是：

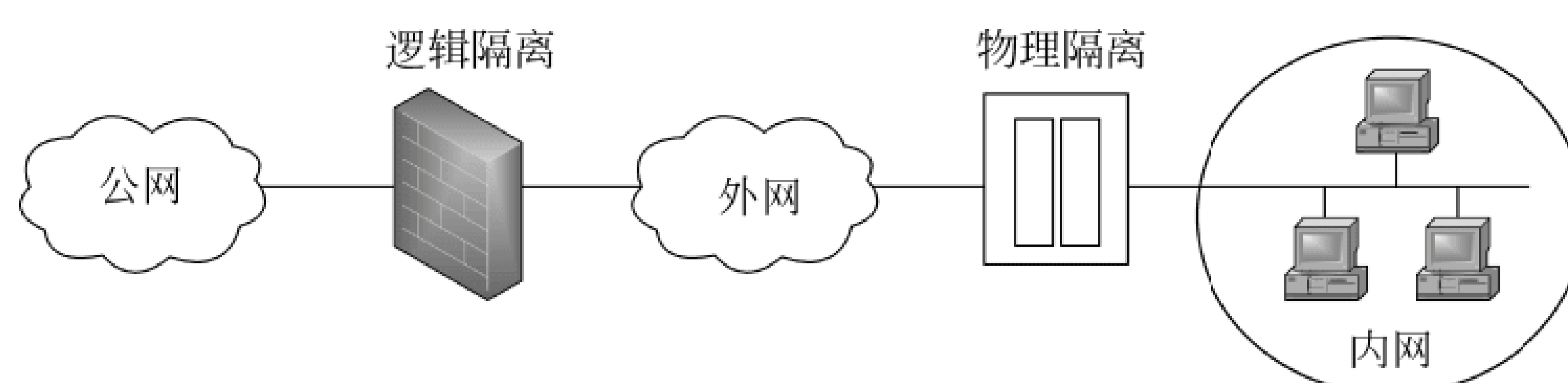


图 7.19　电子政务的三级网络

- 在公网和外网之间实行逻辑隔离；
- 在内网和外网之间实行物理隔离。

所谓物理隔离，是指内部网络与外部网络在物理上没有相互连接的通道，两个系统在物理上完全独立。目前，已经开发出如下几种物理隔离技术。

1. 网络安全隔离卡技术

网络安全隔离卡是一个硬件插卡，可以在物理上将计算机划分成两个独立的部分，每一部分都有自己的“虚拟”硬盘。网络安全隔离卡设置在 PC 最低层的物理部件上，卡的一边通过 IDE 总线连接主板，另一边连接 IDE 硬盘。PC 的硬盘被分割成两个物理区：

- 安全区，只与内部网络连接；
- 公共区，只与外部网络连接。

如图 7.20 所示，网络安全隔离卡就像一个分接开关，在 IDE 硬件层上，由固件控制磁盘通道，任何时刻计算机只能与一个数据分区以及相应的网络连通。于是计算机也因此被分为安全模式和公共模式，并且某一时刻只可以在一个模式下工作。

- 在安全状态时，主机只能使用硬盘的安全区与内部网连接，此时外部网是断开的，硬盘的公共区也是封闭的；
- 在公共状态时，主机只能使用硬盘的公共区与外网连接，此时与内网是断开的，且硬盘的安全区是封闭的。

两个模式转换时，所有的临时数据都会被彻底删除。

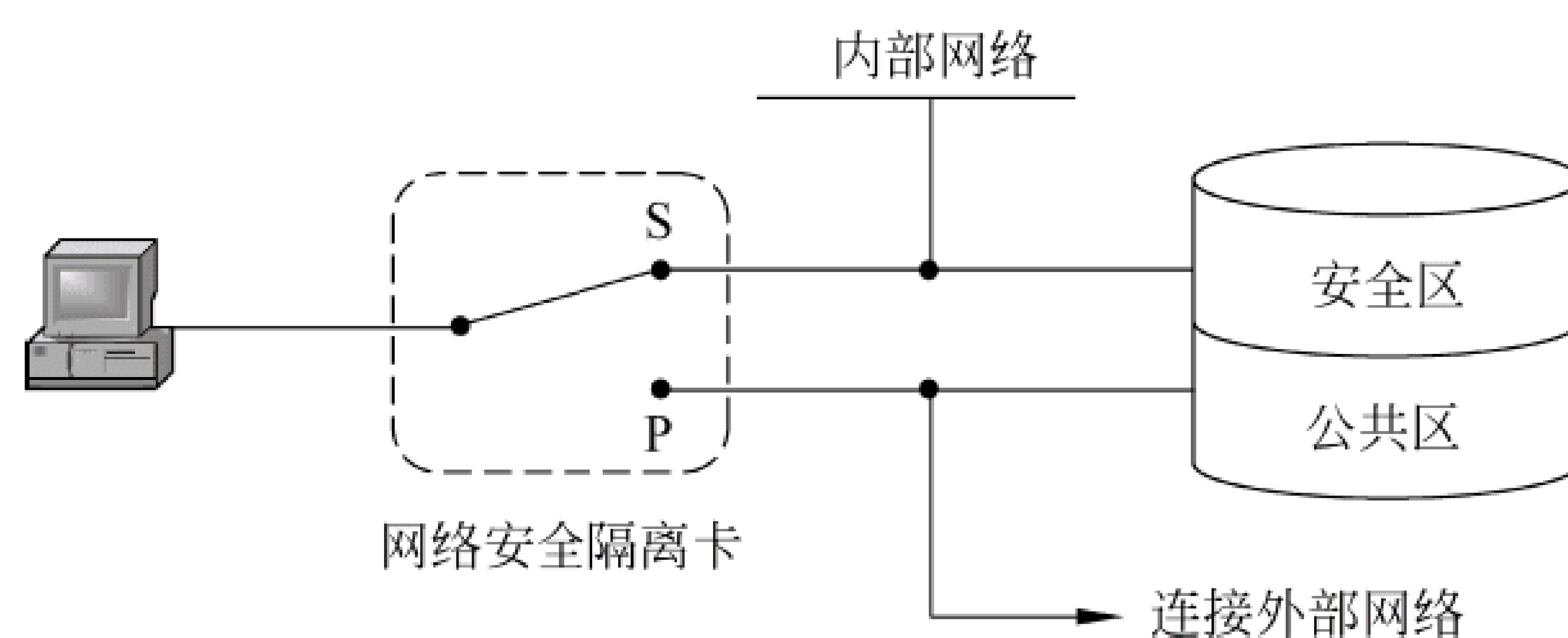


图 7.20　网络安全隔离卡的工作方式

两个状态各有自己独立的操作系统，并分别导入，保证两个硬盘不会同时被激活。两个分区不可以直接交换数据，但是可以通过专门设置的中间功能区进行，或通过设置的安全通道使数据由公共区向安全区转移（不可逆向）。

在安全区及内网连接状态下可以禁用软驱、光驱等移动存储设备，防止内部数据泄密。要转换到公共环境时，须进行如下操作：

- 按正常方式退出操作系统；
- 关闭计算机；
- 将安全硬盘转换为公共硬盘；
- 将 S/P 开关转换到公共网络。

当然，这些操作是由网络安全隔离卡自动完成的。为了便于用户从 Internet 上下载数据，特设了硬盘数据交换区，通过读写控制只允许数据从外网分区向内网分区单向流动。

2. 隔离集线器技术

如图 7.21 所示，网络安全集线器是一种多路开关切换设备。它与网络安全隔离卡配合使用，并通过对网络安全隔离卡上发出的特殊信号的检测，识别出所连接的计算机，自动将其网线切换到相应的网络集线器上，从而实现多台独立的安全计算机与内、外两个网络的安全连接与自动切换。

如果没有检测到来自网络安全隔离卡的信号，两个网络都会被切断。这就减少了安全区的工作站被错误地连上未分类网络的风险。

这种网络安全隔离集线器与数据安全保护器的设置，允许用户顺利地进行额外的网络

工作，并且操作是全透明的，对以太网/快速以太网的标准通信没有任何影响。

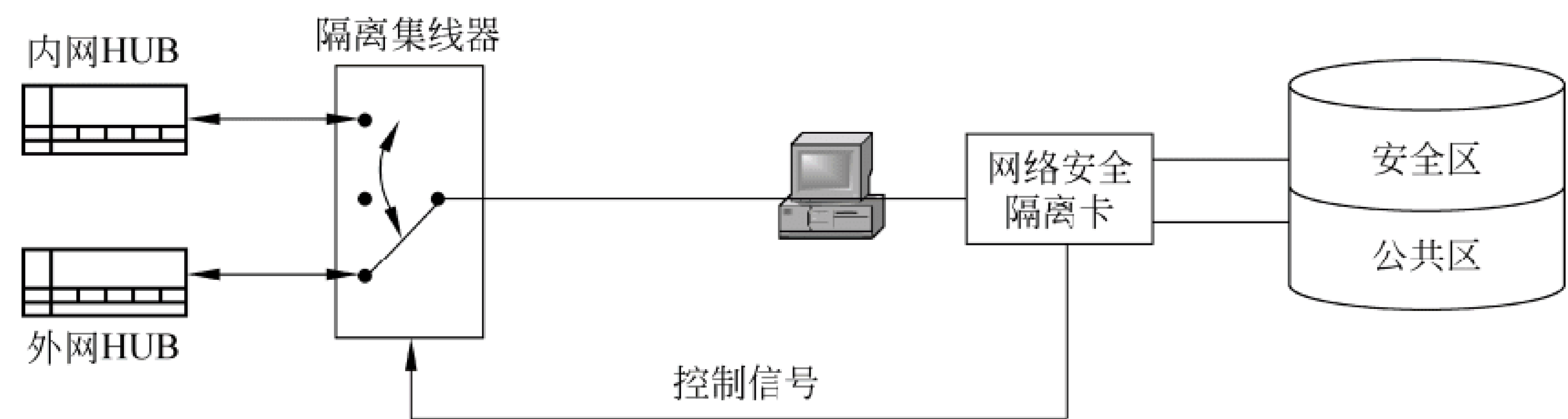


图 7.21　网络安全集线器的工作原理

3. 单主板隔离计算机技术

单主板隔离计算机技术的核心是双硬盘技术，它将内外网转换功能做入 BIOS 中，并将插槽也分为内网和外网。使用方便且安全，价格介于双主机与隔离卡之间。

这种安全计算机是在较低层的 BIOS 上开发的。BIOS 提供信息发送和输出设备的控制，并在 PC 主板上形成两个各自独立的由网卡和硬盘构成的网络接入和信息存储环境，并且只能在相应的网络环境下工作，不可能在一种环境下使用另一种环境下才能使用的设备，包括：

（1）对软驱、光驱提供功能限制，在系统引导时不允许驱动器中有移动存储介质。双网计算机提供软驱关闭/禁用控制。

（2）提供双端口设备（打印机接口/并行接口、串行接口、USB 接口、MIDI 接口等）限制。对于 BIOS 则由防写跳线防止病毒、非法刷新、破坏等。

7.6　网络入侵威慑

从安全性的角度看，所有试图破坏系统安全性的行为都称为攻击，入侵就是成功的攻击。当一次攻击成功的时候，一次入侵就发生了。或者说，系统借以保障安全的第一道防线已经被攻破了。所以，只从防御的角度被动地构筑安全系统是不够的。

安全监控是一种积极的防御措施。它通过对系统中所发生的现象的记录，分析系统出现了什么异常，以便采取相应的对策。

7.6.1　安全审计

1. 安全审计及其功能

虚拟的数字世界是十分脆弱的。随着对它们的依赖程度的增加，不安全感也随之增加。信息被篡改、信息被泄露、身份被伪冒……频发，要求对系统安全方案中的功能提供持续的评估。这就是安全审计。据专家的预测，安全审计技术将成为与防火墙技术、IDS 技术一样的网络安全工具之一。

具体来说，安全审计应当具有下面的功能：

（1）记录关键事件。关于关键事件的界定由安全管理员决定。

（2）对潜在的攻击者进行威慑或警告。

（3）为系统安全管理员提供有价值的系统使用日志，帮助系统管理员及时发现入侵行为和系统漏洞，使安全管理员可以知道如何对系统安全进行加强和改进。

（4）为安全管理员提供一组可供分析的管理数据，用于发现何处有违反安全方案的事件，并可以根据实际情形调整安全政策。

关于安全审计，美国国家标准《可信计算机系统评估超标准》（Trusted Computer System Evaluation Criteria）给出的定义是：一个安全的系统中的安全审计系统，是对系统中任一或所有安全相关事件进行记录、分析和再现的处理系统。它通过对一些重要的事件进行记录，从而在系统发现错误或受到攻击时能定位错误和找到攻击成功的原因，并且是事故后调查取证的基础，当然也是对信息系统的信心保证。

可以看出，安全审计和报警是不可分割的。安全审计由各级安全管理机构实施并管理，并只在定义的安全策略范围内提供。它允许对安全策略的充分性进行评价，帮助检测安全违规，对潜在的攻击者产生威慑。但是，安全审计不直接阻止安全违规。安全报警是由个人或进程发出的，一般在安全相关事件达到某一或一些预定义的阈值时发出。在这些事件中，一些需要立即采取矫正行动，另一些则有进一步研究价值。

2. 安全审计日志

审计日志是记录信息系统安全状态和问题的原始数据。理想的日志应当包括全部与数据以及系统资源相关事件的记录。但这样付出的代价太大。为此，日志的内容应当根据安全目标和操作环境单独设计。典型的日志内容有：

- 事件的性质——数据的输入和输出，文件的更新（改变或修改），系统的用途或期望；
- 全部相关标识——人、设备和程序；
- 有关事件的信息——日期和时间，成功或失败，涉及因素的授权状态，转换次数，系统响应，项目更新地址，建立、更新或删除信息的内容，使用的程序，兼容结果和参数检测，侵权步骤等。对大量生成的日志要适当考虑数据的保存期限。

3. 安全审计的类型

1）根据审计的对象分类

根据审计的对象，安全审计可以分为以下一些类型：

（1）操作系统的审计；

（2）应用系统的审计；

（3）设备的审计；

（4）网络应用的审计。

2）审计的关键部位

通常审计的关键部位有：

（1）对来自外部攻击的审计；

（2）对来自内部攻击的审计；

（3）对电子数据的安全审计。

7.6.2 入侵检测

1. 入侵检测与入侵检测系统

入侵检测系统（Intrusion Detection System, IDS）是对计算机和网络系统资源上的恶意行为进行识别和响应的处理系统；它像雷达警戒一样，在不影响网络性能的前提下，对网络进行警戒、监控；从计算机网络的若干关键点收集信息，通过分析这些信息，看看网络中是否有违反安全策略的行为和遭到攻击的迹象；从而扩展了系统管理员的安全管理能力，提高了信息安全基础结构的完整性。

这里，“入侵”（Intrusion）是一个广义的概念，不仅包括发起攻击的人（包括黑客）取得超出合法权限的行为，也包括收集漏洞信息，造成拒绝访问（Denial of Service）等对系统造成危害的行为。而入侵检测（Intrusion Detection）就是对入侵行为的发觉。它通过对计算机网络等信息系统中若干关键点的有关信息的收集和分析，从中发现系统中是否存在有违反安全规则的行为和被攻击的迹象。入侵检测系统就是进行入侵检测的软件和硬件的组合。

入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，被认为是防火墙后面的第二道安全防线。

具体说来，入侵检测系统的主要功能有：

- 监视并分析用户和系统的行为；
- 审计系统配置和漏洞；
- 评估敏感系统和数据的完整性；
- 识别攻击行为、对异常行为进行统计；
- 自动收集与系统相关的补丁；
- 审计、识别、跟踪违反安全法规的行为；
- 使用诱骗服务器记录黑客行为；

……

2. 实时入侵检测和事后入侵检测

实时入侵检测在网络的连接过程中进行，通过攻击识别模块对用户当前的操作进行分析，一旦发现攻击迹象就转入攻击处理模块，如立即断开攻击者与主机的连接、收集证据或实施数据恢复等。如图 7.22 所示，这个检测过程是反复循环进行的。

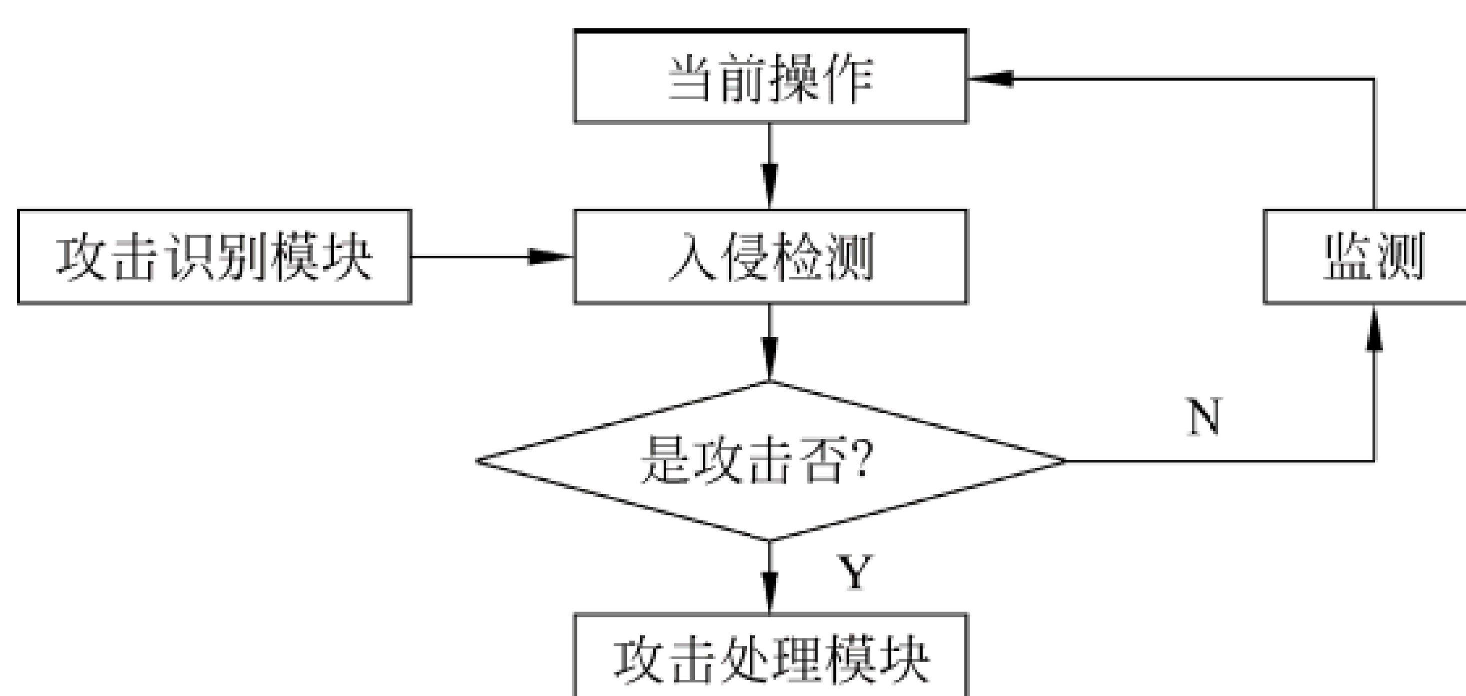


图 7.22　实时入侵检测过程

事后入侵检测是根据计算机系统对用户操作所做的历史审计记录，判断是否发生了攻击行为，如果有，则转入攻击处理模块处理。事后入侵检测通常由网络管理人员定期或不定期地进行的。图 7.23 为事后入侵检测的过程。

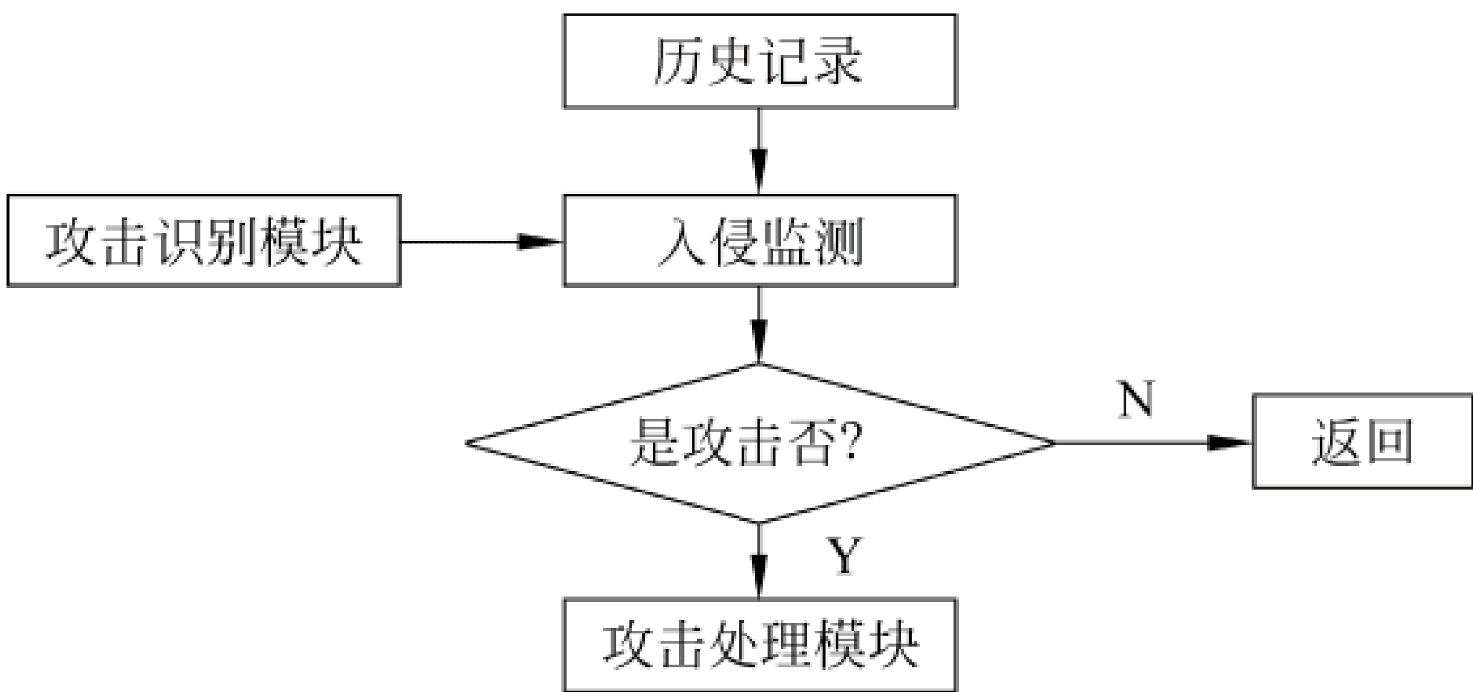


图 7.23　事后入侵检测的过程

3. 入侵检测系统的基本结构

入侵检测是防火墙的合理补充，帮助系统对付来自外部或内部的攻击，扩展了系统管理员的安全管理能力（如安全审计、监视、攻击识别及其响应），提高了信息安全基础结构的完整性。如图 7.24 所示，入侵检测系统的主要工作就是从信息系统的若干关键点上收集信息，然后分析这些信息，用来得到网络中有无违反安全策略的行为和遭到袭击的迹象。

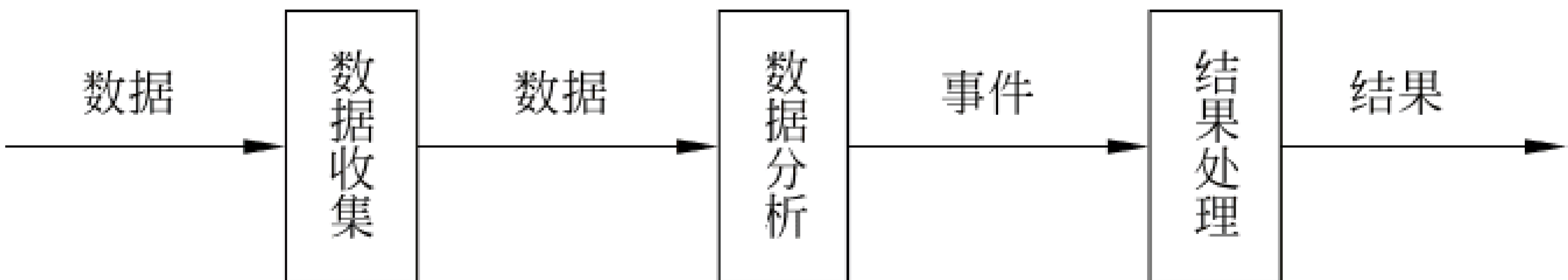


图 7.24　入侵检测系统的通用模型

入侵检测系统这个模型比较粗略。但是它表明数据收集、数据分析和处理响应是一个入侵检测系统的最基本部件。

1）信息收集

入侵检测的第一步是在信息系统的一些关键点上收集信息。这些信息就是入侵检测系统的输入数据。入侵检测系统收集的数据一般有如下 4 个方面：

（1）主机和网络日志文件。主机和网络日志文件中记录了各种行为类型，每种行为类型又包含不同的信息，例如记录“用户活动”类型的日志，就包含登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容。这些信息包含了发生在主机和网络上的不寻常和不期望活动的证据，留下黑客的踪迹。通过查看日志文件，能够发现成功的入侵或入侵企图，并很快地启动响应的应急响应程序。因此，充分利用主机和网络日志文件信息是检测入侵的必要条件。

（2）目录和文件中的不期望改变。网络环境中的文件系统包含很多软件和数据文件。包含重要信息的文件和私密数据的文件经常是黑客修改或破坏的目标。黑客经常替换、修改和破坏他们获得访问权的系统中的文件，同时为了隐蔽他们在系统中活动痕迹，还会尽力替换系统程序或修改系统日志文件。因此，目录和文件中的不期望改变（包括修改、创建和删除），特别是那些正常情况下限制访问的对象，往往就是入侵产生的指示和信号。

（3）程序执行中的不期望行为。每个在系统上执行的程序由一到多个进程来实现。每

个进程都运行在特定权限的环境中。这些环境权限控制着进程可访问的系统资源、程序和数据文件等；操作执行的方式不同，利用的系统资源也就不同。各个进程的行为由它所执行的操作表现。操作包括计算、文件传输、设备以及与网络间其他进程的通信。黑客可能会将程序或服务的运行分解，从而导致它的失败，或者是以非用户或管理员意图的方式操作。因此，若一个进程出现了不期望的行为，则可能表明黑客正在入侵当前的系统。

（4）物理形式的入侵信息。黑客总是想方设法（如通过网络上的由用户私自加上去的不安全——未授权设备）去突破网络的周边防卫，以便能够在物理上访问内部网，在内部网上安装他们自己的设备和软件。例如，用户在家里可能安装 Modem 以访问远程办公室，那么这一拨号访问就成了威胁网络安全的后门。黑客就会利用这个后门来访问内部网，从而越过了内部网络原有的防护措施，然后捕获网络流量，进而攻击其他系统，并偷取敏感的私有信息等等。

2）数据分析

数据分析是 IDS 的核心，它的功能就是对从数据源提供的系统运行状态和活动记录进行同步、整理、组织、分类以及各种类型的细致分析，提取其中包含的系统活动特征或模式，用于对正常和异常行为的判断。

入侵检测系统的数据分析技术依检测目标和数据属性，分为异常发现技术和模式发现技术两大类。

3）响应

早期的入侵检测系统的研究和设计，把主要精力放在对系统的监控和分析上，而把响应的工作交给用户完成。现在的入侵检测系统都提供有响应模块，并提供主动响应和被动响应两种方式。一个好的入侵检测系统应该让用户能够裁减定制其响应机制，以符合特定的需求环境。

在主动响应系统中，系统将自动或以用户设置的方式阻断攻击过程或以其他方式影响攻击过程，通常可以选择的措施有：

- 针对入侵者采取的措施；
- 修正系统；
- 收集更详细的信息。

在被动响应系统中，系统只报告和记录发生的事件。

4. 入侵检测器的部署

入侵检测器是入侵检测系统的核心。入侵检测器部署的位置，直接影响入侵检测系统的工作性能。在规划一个入侵检测系统时，首先要考虑入侵检测器的部署位置。显然，在基于网络的入侵检测系统和基于主机的入侵检测系统中，部署的策略不同。

1）在基于网络的入侵检测系统中部署入侵检测器

基于网络的入侵检测系统主要检测网络数据报文，因此一般将检测器部署在靠近防火墙的地方。具体做法有如图 7.25 所示的几个位置。

（1）DMZ 区内。在这里，可以检测到的攻击行为是：所有针对向外提供服务的服务器的攻击。由于 DMZ 中的服务器是外部可见的，因此在这里检测最为需要。同时，由于 DMZ

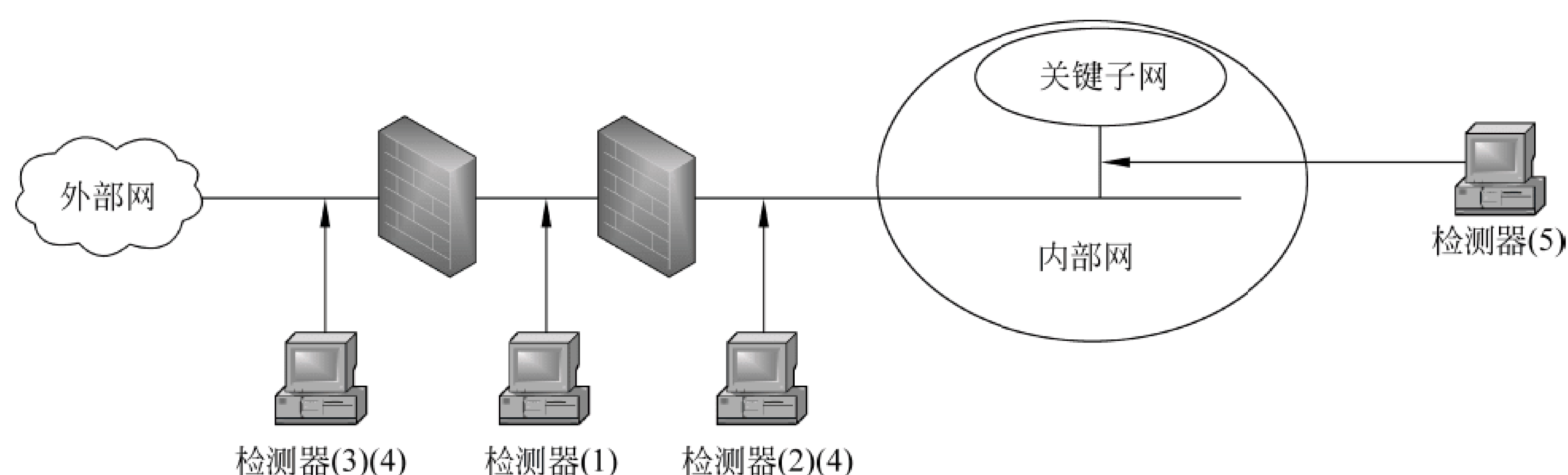


图 7.25　基于网络的入侵检测器的部署

中的服务器有限，所以针对这些服务器的检测，可以使入侵检测器发挥最大优势。但是，在 DNZ 中，检测器会暴露在外部，而失去保护，遭受攻击，导致无法工作。

（2）内网主干（防火墙内侧）。将检测器放到防火墙的内侧，有如下几点好处：

- 检测器比放在 DMZ 中安全。
- 所检测到的都是已经渗透过防火墙的攻击行为。从中可以有效地发现防火墙配置的失误。
- 可以检测到内部可信用户的越权行为。
- 由于受干扰的机会少，报警几率也低。

（3）外网入口（防火墙外侧）。优势是：

- 可以对针对目标网络的攻击进行计数，并记录最为原始的数据包。
- 可以记录针对目标网络的攻击类型。

但是，不能定位攻击的源和目的地址，系统管理员在处理攻击行为上也有难度。

（4）在防火墙的内外都放置。这种位置可以检测到内部攻击，又可以检测到外部攻击，并且无须猜测攻击是否穿越防火墙。但是，开销较大。在经费充足的情况下是最理想的选择。

（5）关键子网。这个位置可以检测到对系统关键部位的攻击，将有限的资源用在最值得保护的地方，获得最大效益/投资比。

2）基于主机的入侵检测系统中部署入侵检测器

基于主机的入侵检测系统通常是一个程序。在基于网络的入侵检测器的部署和配置完成后，基于主机的入侵检测将部署在最重要、最需要保护的主机上。

7.6.3　网络诱骗

防火墙以及入侵检测都是被动防御技术，而网络诱骗是一种主动防御技术。

1. 蜜罐主机技术

网络诱骗技术的核心是蜜罐（Honey Pot）。它是运行在 Internet 上的充满诱惑力的计算机系统。这种计算机系统有如下一些特点：

（1）蜜罐是一个包含有漏洞的诱骗系统，它通过模拟一个或多个易受攻击的主机，给攻击者提供一个容易攻击的目标。

（2）蜜罐不向外界提供真正有价值的服务。

（3）所有与蜜罐的连接尝试都被视为可疑的连接。

这样，蜜罐就可以实现如下目的：

- 引诱攻击，拖延对真正有价值目标的攻击；
- 消耗攻击者的时间，以便收集信息，获取证据。

下面介绍蜜罐的三种主要形式。

1）空系统

空系统是一种没有任何虚假和模拟环境的完全真实的计算机系统，但是有真实的操作系统和应用程序，也有真实的漏洞。这是一种简单的蜜罐主机。

但是，空系统（以及模拟系统）会很快被攻击者发现，因为他们会发现这不是期待的目标。

2）镜像系统

建立一些提供 Internet 服务的服务器镜像系统，会让攻击者感到更真实，也就更具有欺骗性。另一方面，由于是镜像系统，所以比较安全。

3）虚拟系统

虚拟系统是在一台真实的物理机器上运行一些仿真软件，模拟出多台虚拟机，构建多个蜜罐主机。这种虚拟系统不但逼真，而且成本较低，资源利用率较高。此外，即使攻击成功，也不会威胁宿主操作系统安全。

2. 蜜网技术

蜜网（Honey Net）技术也称陷阱网络技术。它由多个蜜罐主机、路由器、防火墙、IDS、审计系统等组成，为攻击者制造一个攻击环境，供防御者研究攻击者的攻击行为。

1）第一代蜜网

图 7.26 为第一代蜜网结构图。

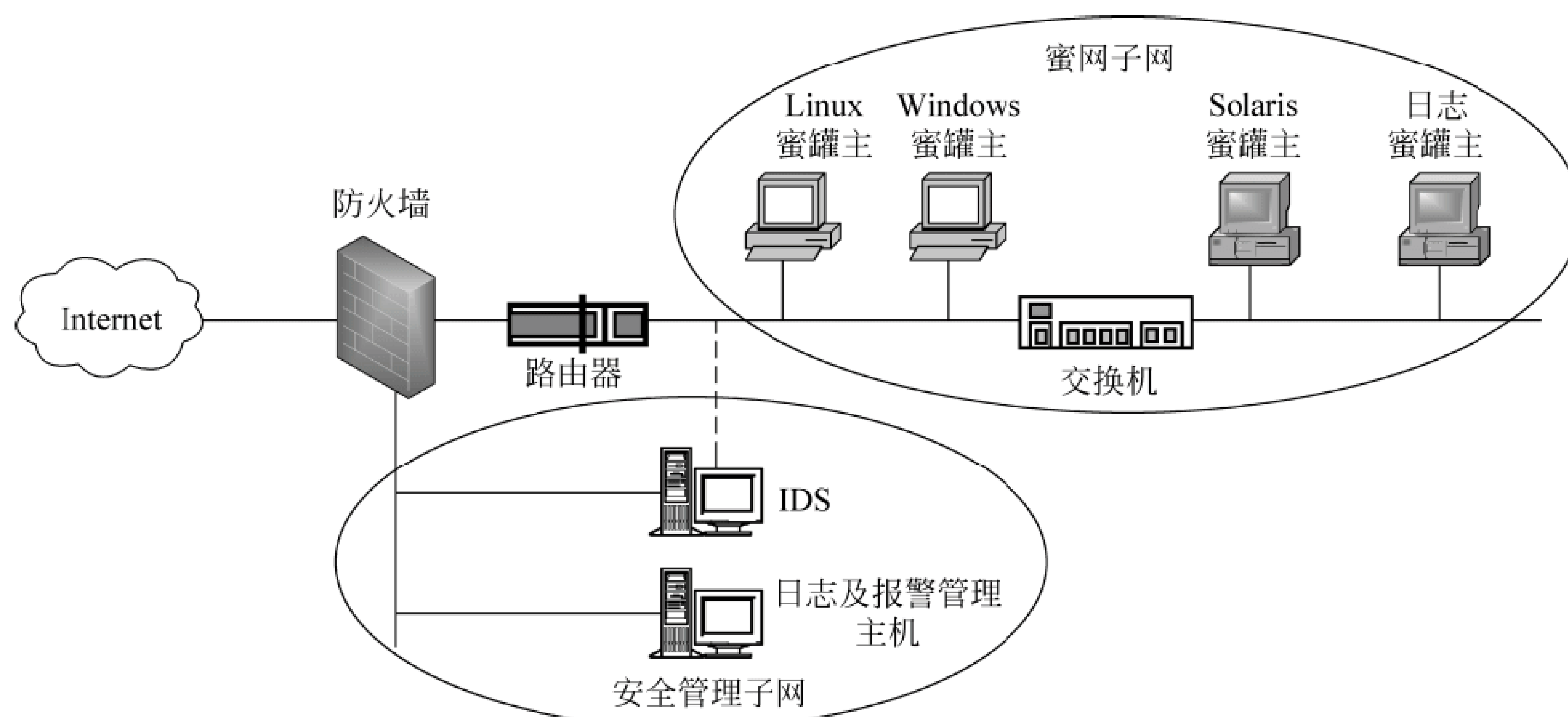


图 7.26　第一代蜜网结构

下面对其中各部件的作用加以介绍。

（1）防火墙。防火墙隔离内网和外网，防止入侵者以蜜网作为跳板攻击其他系统。其配置规则为：不限制外网对蜜网的访问，但需要对蜜罐主机对外的连接予以控制，包括：

- 限制对外连接的目的地；
- 限制蜜罐主机主动对外连接；
- 限制对外连接的协议；

……

（2）路由器。路由器放在防火墙与蜜网之间，利用路由器具有控制功能来弥补防火墙的不足，例如，防止地址欺骗攻击、DoS 攻击等。

（3）IDS。IDS 是蜜网中的数据捕获设备，用于检测和记录网络中可疑通信连接，报警可疑的网络活动。

2）第二代蜜网

图 7.27 为第二代蜜网结构图。

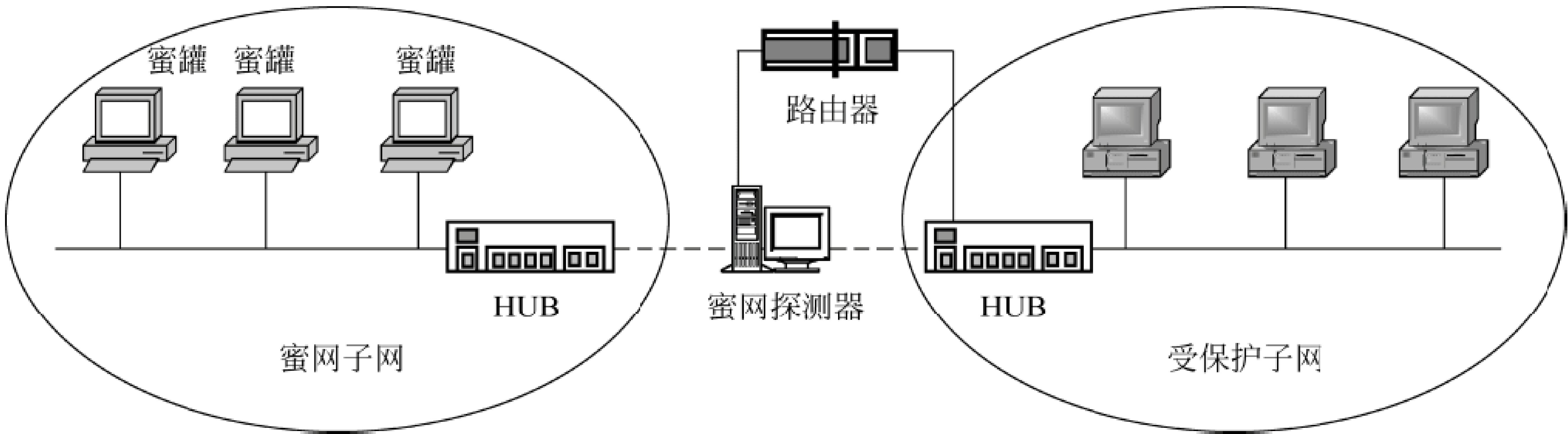


图 7.27　第二代蜜网结构

第二代蜜网技术将数据控制和数据捕获集中到蜜网探测器中进行，所带来的好处是：

- 便于安装和管理；
- 隐蔽性更强；
- 可以监控非授权活动；
- 可以采取积极的响应方法限制非法活动的效果，如修改攻击代码字节、使攻击失效等。

3）第三代蜜网

第三代蜜网是目前正在开发的蜜网技术。它是建立在一个物理的设备上的分布式虚拟系统。如图 7.28 所示，这样就把蜜罐、数据控制、数据捕获、数据记录等，都集中到一台物理的设备上。

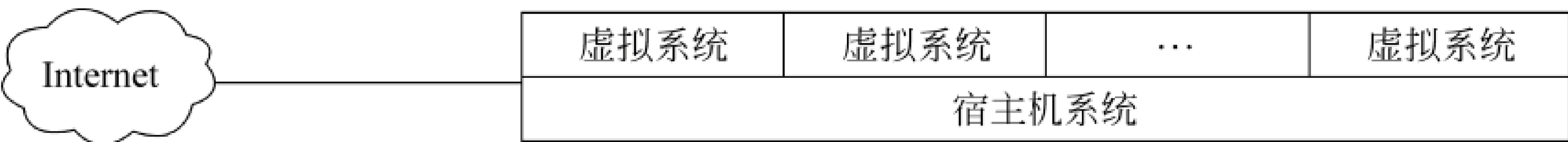


图 7.28　第三代蜜网结构

7.7　信息网络安全的法律与法规

Internet 的普及与发展将日益渗透到人类社会的各个方面，改变人们的工作方式、学习方式、思维方式和生活方式。这些方式的改变，已经给人类社会带来了一系列的深刻影响，

引发了一系列新的社会问题，要求社会建立或调整相应的行为道德规范和法律制度，从伦理和法制两个方面约束人们的行为，协调人们在新时期的利益和关系。行为规范与信息立法是维护 Internet 秩序的措施。随着 Internet 对社会活动产生越来越大的影响，各国政府和有关组织都在积极进行这方面的研究，有的已经采取了相应的对策。

美国参议院 1995 年 6 月通过《计算机庄严法》（CDA）。

欧盟委员会 1996 年 10 月 16 日通过了《Internet 有害与违法信息通信》和《在新的电子信息环境中保护未成年人和人的尊严》绿皮书。

德国已经起草了《信息和通信服务联邦法案》。

日本的 ISP 自发地制定了《Internet 事业伦理准则》。

20 世纪 90 年代起，我国先后颁布了《中国公众多媒体通信管理办法》（1997 年 12 月 1 日）、《中华人民共和国计算机信息网络国际联网管理暂行规定》（1996 年 2 月 1 日）、《中国互联网络域名注册暂行管理办法》、《中国互联网络域名注册实施细则》等。进入 21 世纪，我国的信息立法进一步加强：2000 年 9 月 25 日，《中华人民共和国电信条例》、《互联网信息服务管理办法》出台，2000 年 11 月 1 日，中国互联网络信息中心（CNNIC）发布《中文域名注册管理办法》，2000 年 11 月 6 日，信息产业部颁布了《互联网电子公告服务管理规定》，同时国务院新闻办公室和信息产业部联合颁布了《互联网站从事登载新闻业务管理暂行规定》。

信息立法与政策法规应该考虑一个国家的特殊背景与需要。在法制体系已经比较健全的国家，可以只对原来的法律做一些补充性规定即可；在法律机制比较薄弱的国家，则需要对法律基础设施做大量的工作。信息立法涉及的范围较广，但一般应当包括：

- 信息表达的权利和义务；
- 信息获取的权利和义务；
- 信息保存的权利和义务；
- 信息传递的权利和义务；
- 信息资源分配的权利和义务；
- 信息搜集和处理的权利和义务；
- 利用信息和信息基础设施的权利和义务。

下列 15 种互联网犯罪将会被追究刑事责任：

（1）违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统；

（2）制作、传播计算机病毒，设置破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损坏；

（3）违反国家规定，擅自中断信息网络或者通信服务，造成信息网络或通信系统不能正常运行；

（4）利用互联网造谣、诽谤或者发表、传播其他信息，煽动颠覆国家政权、推翻社会主义制度，或者煽动分裂国家、破坏国家统一；

（5）利用互联网窃取、泄露国家秘密、情报或者军事秘密；

（6）利用互联网煽动民族仇恨、民族歧视，破坏民族团结；
（7）利用互联网组织邪教组织、联络邪教组织成员，破坏国家法律、行政法规实施；
（8）利用互联网进行诈骗、盗窃；
（9）利用互联网销售伪劣产品或者对商品、服务进行虚假宣传；
（10）利用互联网编造并传播影响证券和期货交易的虚假宣传；
（11）在互联网上建立淫秽站点链接服务，或者传播淫秽书刊、影片、音乐、图片；
（12）利用互联网侮辱他人或者捏造事实诽谤他人；
（13）非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密；
（14）利用互联网侵犯他人知识产权；
（15）利用互联网损害他人商业信誉和商品信誉。

实验 18　实现一个 VPN 连接

一、实验目的

（1）理解 VPN 的工作原理。
（2）了解 VPN 的应用。
（3）掌握 VPN 实现的技术方法。

二、实验内容

（1）实验一个 VPN 连接。
（2）测试连接后的 VPN 网络。

三、建议环境

（1）在 Windows 操作系统中利用 PPTP 配置 VPN 网络，即在 Windows 2000 Server 中选择“开始”→“程序”→“管理工具”命令，单击“路由和远程访问”选项，进行配置。

（2）在 Windows 中配置 IPSec，即选择“开始”→“程序”→“管理工具”命令，进入“本地安全策略”界面；在右侧窗口中，可以看到默认情况下 Windows 内置的“安全服务器”“客户端”“服务器”3 个安全选项，并附有描述。

（3）在 Linux 操作系统中利用 CIPE 配置 VPN。CIPE（Crypto IP Encapsulation）是主要为 Linux 而开发的 VPN 实现软件。CIPE 使用默认的 CIPE 加密机制（标准的 Blowfish 或 IDEA 加密算法）来加密 IP 分组，并把这些分组添加目标头信息后，封装或“包围”在数据报（UDP）中。然后，这些 UDP 分组再通过 CIPE 虚拟网络设备（cipcbx）和 IP 层。

四、实验准备

（1）对要使用的 VPN 连接进行需求分析。
（2）根据需求分析提出使用的 VPN 连接方案。
（3）设计实现确定的 VPN 方案所需要的软硬件环境。
（4）设计进行 VPN 连接的步骤。
（5）设计进行 VPN 连接测试的方法和步骤。

五、推荐的分析讨论内容

（1）搜集各种 VPN 实现技术，并进行比较。
（2）对自己实现的 VPN 进行安全风险分析，提出改进设想。
（3）有的计算机网络具有单入口点，即出入网络的所有数据都只通过单个网关（路由器和/或防火墙），而有的网络中使用了多个网关。那么在这两种情况下，进行 VPN 配置有什么区别？
（4）其他发现或想到的问题。

实验 19　个人软件防火墙设置

一、实验目的

个人防火墙是为解决网络上黑客攻击问题而研制的个人信息安全产品，具有比较完备的规则设置，能够有效地监控大多数网络连接，保护网络不受黑客的攻击。

防火墙有软件防火墙和硬件防火墙。软件防火墙不需要额外投资，适合于家庭 PC 上网使用。在学习计算机网络安全时，通过它也可以初步领略防火墙的 ACL 设置和包过滤规则的设置方法和意义。

二、实验环境

（1）两台已经上网的计算机。
（2）瑞星个人软件防火墙。

三、实验准备

1. 了解软件防火墙的下载和安装方法

（1）瑞星个人防火墙是一款免费防火墙。进入瑞星官网（如图 7.29 所示）或其他相关下载网站，都可以看到有关免费下载的提示。

（2）依照向导提示，可以完成下载。下载后，有安装提示，如图 7.30 所示。



图 7.29　瑞星官网



图 7.30　瑞星个人防火墙的安装提示

2. 了解产品功能

安装之后，就会生成一个快捷图标，单击这个图标，就会进入瑞星个人防火墙工作主界面，如图 7.31 所示。

这个主界面可以分为 6 个区域：重要功能、流量显示、版本信息、配置菜单、网络信息、产品宣传。这里主要关心的是重要功能区和配置菜单区。而重要功能部分的设置就是选择开启与关闭，非常简单。下面主要介绍配置菜单区的一些功能。

（1）网络安全页面。单击“网络安全”图标，可以弹出如图 7.32 所示的窗口。这个窗口中罗列了常用的一些攻击的拦截选项供用户选择。



图 7.31　瑞星个人防火墙主页



图 7.32　瑞星个人防火墙的“网络安全”页面

（2）家长控制页面。家长控制页面主要用于对自制力差者使用计算机的控制。在这个页面中，控制人设置密码，以管理不同人使用时的规则开启或关闭。如图 7.33 所示为开启状态。只有在开启状态才能对规则进行选择或修改。规则内容包括日期/时间控制和上网策略控制，这些只要简单选择即可。另外，控制者还可以另外制定控制策略。



图 7.33　瑞星个人防火墙的“家长控制”页面

（3）小工具。小工具为用户提供了一些修理维护工具，如图 7.34 所示。



图 7.34　瑞星个人防火墙的“小工具”页面

（4）防火墙规则页面。这个页面分为两个子页面：“联网程序规则”和“IP 规则”。

图 7.35 是“联网程序规则”子页面。这个页面用于内部程序对外部的访问，也可以看成是一种 ACL。在这个页面中，用户可以对所需程序进行选择，并在该项后面进行“放行”或“阻止”的选择。这实际上是黑名单或白名单的确定。这些规则允许删除、修改，也可以另外增加、导入或导出。图 7.36 为选中一条规则后，单击“修改”按钮后弹出的修改子页面。



图 7.35 “防火墙规则”页面的子页面——“联网程序规则”

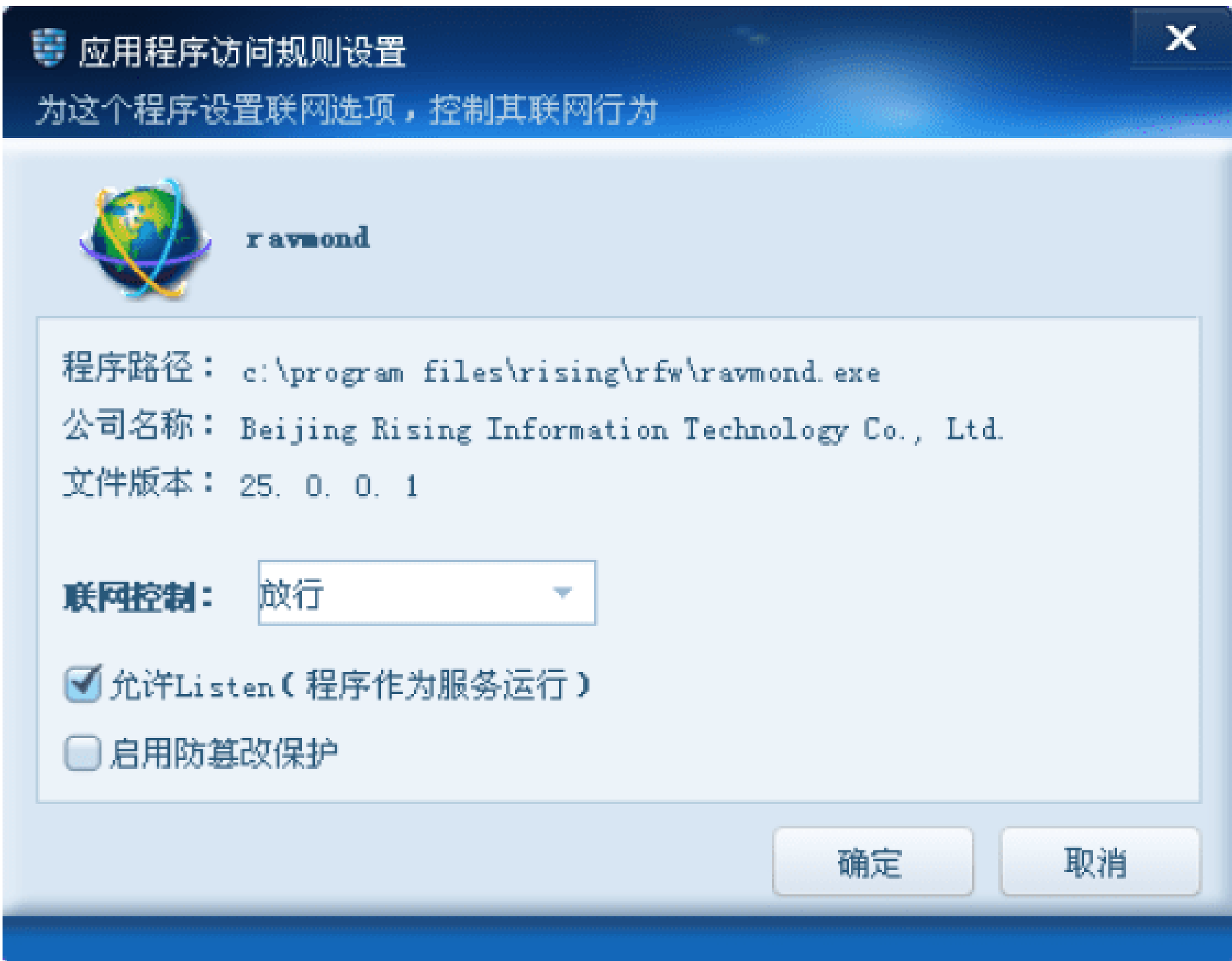


图 7.36 “联网程序规则”的修改子页面

图 7.37 为“IP 规则”子页面。其操作与“联网程序规则”类似，只是用于控制外部对内部的访问，是一种包过滤机制。图 7.38 为其“修改”子页面。



图 7.37 “防火墙规则”页面的子页面——“IP 规则”

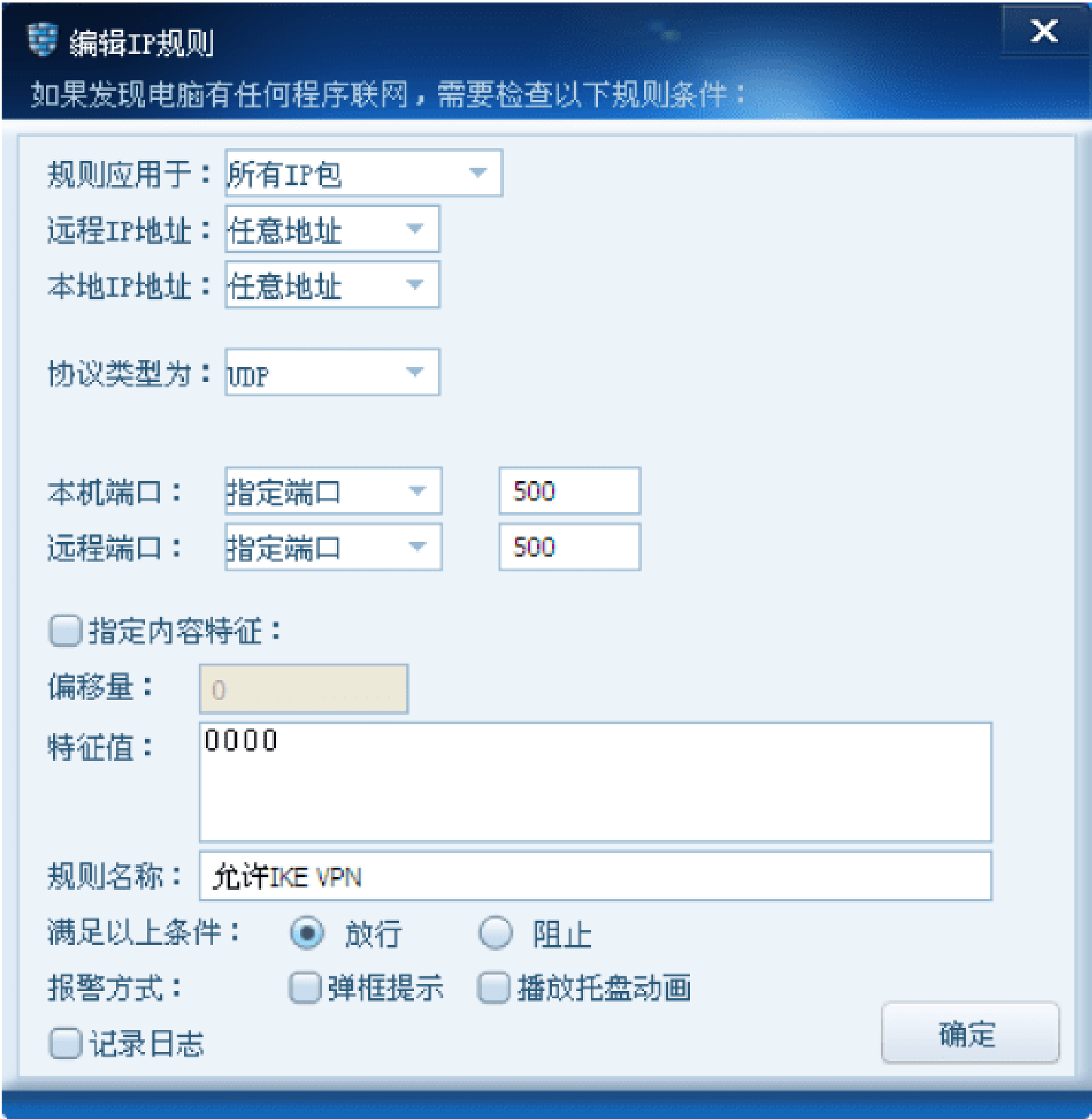


图 7.38 “联网程序规则”的修改子页面

3. 制定防火墙规则

（1）家长控制规则。

（2）联网程序规则。

（3）额外的实验——在上述基本实验之外，自己设想的其他内容。

（4）IP 规则。

4. 制定测试方法

（1）具体访问方法。

（2）ping 方法。

四、实验过程

（1）下载并安装瑞星个人防火墙。

（2）根据预先制定的规则，进行防火墙设置，记录设置中出现的问题。

（3）用预先制定的测试方法进行测试，记录设置中出现的问题。

（4）额外实验及其测试。

五、分析与讨论

（1）进行 ACL 设置要注意什么？

（2）设置包过滤层规则要注意什么？

（3）这个防火墙有什么地方需要改进？

习　题　7

一、选择题

1. 特洛伊木马攻击的威胁类型属于【　　】。

A. 授权侵犯威胁　　B. 植入威胁　　C. 渗入威胁　　D. 旁路控制威胁

2. 计算机病毒是指能够侵入计算机系统并在计算机系统中潜伏、传播、破坏系统正常工作的一种具有繁殖能力的【　　】。

A. 指令　　B. 程序　　C. 设备　　D. 文件

3. 下列叙述中是数字签名功能的是【　　】。

A. 防止交易中的抵赖行为发生　　B. 防止计算机病毒入侵

C. 保证数据传输的安全性　　D. 以上都不对

4. 某银行为了加强自己网站的安全性，决定采用一个协议，应该采用【　　】协议。

A. FTP　　B. HTTP　　C. SSL　　D. UDP

二、填空题

1. ________是为程序开辟的秘密入口。

2. 在对称型密钥体系中，________和________采用同一密钥。

3．CA的功能是________________________________。

三、简答题

1．试述计算机系统病毒防治的未来对策。

2．举例说明黑客有哪些攻击手段。

3．试述Internet安全问题现状。

4．网络攻击有哪几种类型？

5．对称加密和非对称加密有何不同？

6. 分析消息认证码可能遭受的攻击。

7. 简述数字签名的用途和基本流程。

8. 查阅相关资料，比较各种数字签名算法的优缺点。

9. 数字签名进程需要哪些数据？

10. 查阅资料，简述有关PKI的标准及其相关产品。

11. PKI可以提供哪些安全服务？PKI体系中包含了哪些与信任有关的概念？

12. 收集国内外有关认证的网站信息，简要说明各网站的特点。

13. 收集国内外有关认证的最新动态。

14. 简述口令可能会遭受哪些攻击。

15. 假定只允许使用26个字母构造口令，在下列情况下各可以构造出多少条口令？

- 口令最多可以使用 n 个字符，$n = 4$，6，8，不区分大小写。
- 口令最多可以使用 n 个字符，$n = 4$，6，8，区分大小写。

16. 编写一个口令生成程序。程序以长度s（可以取$s = 8$，16，32，64）的随机二进制种子作为输入：

- 让多名用户使用你的程序生成口令，记录有多少人选择了相同的事件。
- 生成一个口令并加密。然后让人通过尝试随机数种子的所有值进行口令攻击。事先要给定一个猜测次数的期望值。

17. 简述生物特征认证的发展趋势。

18．什么是VPN？

19. 简述安全审计的作用。

20. 综述入侵检测技术的发展过程，并提出自己的思路。

21. 入侵检测系统有哪些可以利用的数据源？

22. 入侵检测技术与法律有什么关系？

23. 简述蜜罐技术的特殊用途。

24. 收集国内外有关入侵检测、网络诱骗或安全审计的最新动态。

25. 下面是选择防火墙时应考虑的一些因素，请按你的理解，将它们按重要性排序。

- 被保护网络受威胁的程度；
- 受到入侵，网络的损失程度；
- 网络管理员的经验；
- 被保护网络的已有安全措施；

- 网络需求的发展；
- 防火墙自身管理的难易度；
- 防火墙自身的安全性。

26. 简述目前物理隔离产品的特点，并进行优缺点分析。
27. 有哪些网络安全措施具有对网络攻击的威慑作用？

参 考 文 献

[1] 张基温. 计算机网络教程[M]．北京：清华大学出版社，2017．

[2] 张基温，张展赫．计算机网络技术与应用教程[M]．第2版. 北京：人民邮电出版社，2016．

[3] 张基温．计算机网络实训教程[M]．北京：人民邮电出版社，2001．

[4] 张基温．计算机网络技术[M]．北京：高等教育出版社，2004．

[5] 张基温．计算机网络原理[M]．第2版．北京：高等教育出版社，2006．

[6] 谢希仁．计算机网络[M]．第6版．北京：电子工业出版社，2013．

[7] 张基温．信息系统安全教程[M]. 第2版. 北京：清华大学出版社，2015．

[8] http://www.chinaitlab.com．

[9] http://www.e-works.net.cn．

高等教育质量工程·信息技术系列示范教材

系列主编：张基温

- 新概念 C 程序设计大学教程（第 4 版） 张基温 编著
- 新概念 C++程序设计大学教程（第 3 版） 张基温 编著
- 新概念 Java 程序设计大学教程（第 3 版） 张基温 编著
- Python 程序开发 张基温 编著
- 计算机组成原理教程（第 8 版） 张基温 编著
- 计算机组成原理解题参考（第 8 版） 张基温 编著
- 计算机网络教程（第 2 版） 张基温 编著
- 信息系统安全教程（第 3 版） 张基温 编著
- 信息系统安全教程（第 3 版）习题详解 栾英姿 编著
- 大学计算机——计算思维导论（第 2 版） 张基温 编著
- UI 设计教程 牛金巍 编著
- APP 开发教程——HTML5 应用 尹志军 编著